VIVRE À NU

PROJET SUR LA NOUVELLE TRANSPARENCE

Vivre à nu

la surveillance au Canada

Sous la direction de :

COLIN J. BENNETT,

KEVIN D. HAGGERTY,

DAVID LYON,

VALERIE STEEVES


AU PRESS
Athabasca University

Publié par Athabasca University Press
10011, rue 109, bureau 1200, Edmonton (Alberta) T5J 3S8

ISBN 978-1-927356-83-8 (couverture souple) ISBN 978-1-927356-84-5 (pdf) ISBN 978-1-927356-85-2 (epub)
doi : 10.15215/aupress/9781927356838.01

Couverture et mise en pages de Marvin Harder, marvinharder.com
Imprimé et relié au Canada par Friesens

Catalogage avant publication de Bibliothèque et Archives Canada

Vivre à nu : la surveillance au Canada : projet sur la nouvelle transparence / éditeurs, Colin J. Bennett, Kevin D. Haggerty, David Lyon, Valerie Steeves.
Comprend des références bibliographiques et un index.
Publié en formats imprimé(s) et électronique(s).

1. Droit à la vie privée – Canada. 2. Surveillance électronique – Aspect social – Canada. I. Bennett, Colin J. (Colin John), 1955- , éditeur intellectuel de compilation II. Haggerty, Kevin D., éditeur intellectuel de compilation III. Lyon, David, 1948- , éditeur intellectuel de compilation IV. Steeves, Valerie M., 1959- , éditeur intellectuel de compilation
JC596.2.C3V58 2014 323.44'830971 C2013-908689-7
C2013-908690-0

Nous tenons à remercier le gouvernement du Canada de l'appui financier apporté par l'intermédiaire du Fonds du livre du Canada pour l'édition.


Canadian Heritage
Patrimoine canadien

Nous remercions également le gouvernement de l'Alberta de l'aide offerte par l'intermédiaire du Fonds de développement multimédia de l'Alberta.



L'usage du générique masculin a pour seul but d'alléger le texte et d'en faciliter la lecture.

Table des matières

Préface

Vivre à nu : la surveillance au Canada expose neuf grandes tendances qui sont observées dans le traitement des renseignements personnels partout dans le monde. Ces tendances touchent tous les Canadiens, mais peu d'entre eux savent comment, quand et à quelles fins leurs données personnelles sont utilisées par les grandes organisations et quelles sont les conséquences de cette utilisation. Voilà pourquoi cet ouvrage est intitulé *Vivre à nu* ; il démontre que nos vies sont plus que jamais ouvertes et visibles pour les organismes et que cette visibilité a de réels effets sur chaque sphère de notre vie, que nous soyons citoyens, consommateurs, travailleurs ou voyageurs.

Le sous-titre de l'ouvrage traduit bien cette évolution : *La surveillance au Canada*. Par « surveillance », nous entendons *toute approche systématique axée sur les renseignements personnels qui vise à influencer, à gérer, à autoriser ou à contrôler les personnes dont l'information est recueillie.* Que nous obtenions des soins de santé dans une clinique, que nous utilisions une carte de fidélité dans un magasin, que nous accomplissions nos tâches quotidiennes au travail, que nous vérifiions nos messages sur un téléphone intelligent ou que nous fassions la queue à la sécurité pour embarquer dans un avion, nos données sont glanées, stockées, classées, transmises ou même vendues à des tiers de manière à orienter nos achats ou nos choix, à retarder notre départ ou à faire en sorte que nous soyons traités de façon juste ou injuste, récompensés ou punis pour notre comportement.

Plus les organismes prennent le virage numérique, plus ils souhaitent obtenir nos données personnelles pour augmenter leur efficacité, leur productivité, leur supervision et leur contrôle. Les organismes se rendent rapidement compte que leurs initiatives numériques leur permettent d'économiser de l'argent ou d'attirer plus de clients ; ils commencent alors à utiliser davantage les nouvelles technologies et techniques pour cibler des groupes précis de personnes auxquels ils réservent un traitement différent. À titre d'exemple, les cartes de fidélité récompensent les clients fidèles, les prestations d'aide sociale sont ciblées avec précision, la lentille des caméras dans la rue montre de façon disproportionnée les jeunes et les minorités en milieu urbain et une personne qui veut prendre un café peut rapidement trouver le Starbucks le plus proche.

Dans ces exemples, comme dans ceux présentés tout au long de cette publication, la surveillance est perçue comme un outil organisationnel qui entraîne des conséquences ambiguës. Elle n'est ni bonne, ni mauvaise, ni utile, ni dangereuse. Elle n'est aussi jamais neutre. Cet ouvrage mettra en lumière les résultats produits par les grandes tendances observées ; ces résultats exhortent non seulement ceux qui traitent des renseignements de nature délicate, mais également ceux dont les données sont divulguées sur une base quotidienne ou à chaque instant, à porter une attention particulière à l'utilisation des données personnelles. En somme, ce volume vise à attirer l'attention sur des questions pressantes de protection des renseignements, d'équité et de justice.

Quelles sont ces grandes tendances ?

Tendance 1 : **La surveillance augmente rapidement.** Notre nouvelle vie numérique a multiplié de façon spectaculaire les possibilités de surveillance. D'ailleurs, nous pouvons observer facilement cette augmentation dans le quotidien de nos enfants. En constatant à quel point un jeune enfant peut être exposé à la surveillance, on comprend bien que le traitement des données personnelles influence bien des aspects quotidiens de notre vie.

Tendance 2 : **La demande croissante pour un renforcement de la sécurité fait progresser la surveillance.** Cette constatation est évidente dans un aéroport, mais elle s'applique également au maintien de l'ordre et à la surveillance en milieu de travail. Or, il n'est pas clair que cette surveillance permet véritablement de mieux nous protéger.

Tendance 3 : **Les organismes publics et privés sont de plus en plus interreliés.** Alors qu'auparavant la surveillance était effectuée principalement par le gouvernement ou les corps policiers, grâce au recours accru à la sous-traitance les organismes à but lucratif ont fait leur entrée sur l'échiquier de la surveillance. La quantité de données personnelles recueillies par les entreprises dépasse maintenant celle recueillie par les corps policiers et les services de renseignement. D'ailleurs, le gouvernement obtient et traite maintenant des données personnelles contenues dans des bases

de données commerciales, augmentant ainsi considérablement la quantité d'information dont il dispose sur ses citoyens.

Tendance 4 : **Il est de plus en plus difficile de déterminer quelle information est privée et quelle ne l'est pas.** Votre nom ou votre numéro d'assurance sociale permettent de bien vous identifier. Qu'en est-il d'une série de photos dans lesquelles vous apparaissez et qui est publiée sur Facebook ou d'une photo de votre plaque d'immatriculation prise par une caméra sur une autoroute ? Chacune de ces photos peut être utilisée pour vous identifier ou vous suivre. Par ailleurs, on peut faire ce genre d'identification en combinant différentes formes de données.

Tendance 5 : **L'ampleur de la surveillance mobile et de la géolocalisation s'accroît.** De plus en plus d'organismes, des services de police aux responsables-marketing, souhaitent non seulement savoir qui vous êtes (identification) et ce que vous faites (comportement), mais également savoir *où* vous êtes en tout temps. Nos appareils mobiles augmentent notre visibilité.

Tendance 6 : **Les pratiques et les processus de surveillance se mondialisent.** Le Canada est loin d'être le seul pays à connaître une croissance rapide de la surveillance sur son territoire. D'ailleurs, la majeure partie de la surveillance découle de vastes changements aux politiques internationales : par exemple, les transporteurs aériens appliquent des procédures similaires partout dans le monde. Cependant, la façon dont nous faisons face à la surveillance dépend des traditions, des lois et de la culture canadiennes.

Tendance 7 : **La surveillance est maintenant intégrée dans des cadres courants** comme les voitures, les immeubles et les maisons. De plus en plus, des appareils permettant de reconnaître les propriétaires ou les utilisateurs – grâce à des technologies comme des commandes vocales ou la lecture d'une carte – sont ajoutés à ces éléments fondamentaux de la vie. Par conséquent, la surveillance se propage de plus en plus, tout en étant moins perceptible.

Tendance 8 : **Le corps humain est de plus en plus utilisé comme source de surveillance.** De nos jours, l'utilisation des empreintes digitales, de la lecture de l'iris, de la reconnaissance faciale et des registres d'ADN est courante pour identifier les gens. Notre corps sert de mot de passe et les traces délicates qu'il laisse sont parfois

considérées comme étant plus fiables que nos déclarations ou notre historique.

Tendance 9 : **La surveillance sociale s'accroît.** Les médias sociaux ont entraîné une multiplication des occasions et des outils permettant la surveillance numérique. Cette tendance quelque peu différente soulève des questions déroutantes au sujet de la protection des renseignements personnels tout en faisant de la surveillance un phénomène plus normal et moins exceptionnel.

Que peut-on faire ?

Nous ne vivons pas dans un état policier. Le Canada affiche un bilan relativement bon pour ce qui est de limiter la surveillance non nécessaire et de promouvoir la protection des renseignements personnels. Toutefois, au cours des dernières années, des événements comme la création de listes de personnes interdites de vol et l'accès aux renseignements personnels en ligne par les policiers sont venus ternir la réputation du pays. Par ailleurs, les commissariats à la protection de la vie privée (fédéral et provinciaux) font l'envie de nombre de pays et les particuliers autant que les organismes dénoncent régulièrement les manques flagrants de protection des renseignements personnels au Canada.

Dans *Vivre à nu,* nous nous intéressons surtout au traitement non nécessaire, excessif et parfois illégal des données personnelles. Pour s'élever contre la croissance de la surveillance, nous devons soulever des questions au sujet des abus qui découlent d'une application imprudente à d'autres domaines de certaines mesures de surveillance légitimes. On appelle souvent ce phénomène « détournement de fonction » ou « changement d'orientation de la mission ». Bien que certaines mesures de protection générale existent, les principales formes de résistance à la surveillance non désirée ou injustifiée se manifestent lorsqu'un événement précis attire l'attention du public. L'événement ainsi rendu public provoque généralement plusieurs réactions différentes, notamment la prise de recours au titre des lois fédérales et provinciales, de même que l'organisation de manifestations par des citoyens ou des groupes. Chacune de ces réactions peut avoir un effet. Conjuguées, elles peuvent devenir particulièrement puissantes.

Nous disposons de plusieurs acquis pour relever les défis auxquels nous devons faire face. Les Canadiens jouissent d'une solide protection au titre

de la *Charte canadienne des droits et libertés* (1982) , de la *Loi fédérale de 1982 sur la protection des renseignements personnels* (laquelle s'applique au gouvernement) et de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE, 2004) (laquelle s'applique aux entreprises) ainsi que de plusieurs autres lois provinciales. De surcroît, les commissaires à la protection de la vie privée du gouvernement fédéral et des gouvernements provinciaux ont fait preuve de vigilance en s'efforçant de s'assurer que tant l'esprit que la lettre des dispositions législatives sur la protection des renseignements personnels sont respectés. Les professionnels et les organismes non gouvernementaux de la protection de la vie privée ont renforcé les mesures de protection offertes et peuvent agir en tant que dénonciateur dans certains dossiers. Par contre, ces mesures de protection ne peuvent être efficaces que si elles sont appuyées par des citoyens informés et actifs. La population en général, de même que les initiatives de sensibilisation, jouent un rôle crucial en dénonçant la surveillance, en posant des questions et en revendiquant la protection des renseignements personnels.

Dans *Vivre à nu,* nous démontrons de façon radicale à quel point nous sommes devenus visibles pour une myriade d'organismes et nous expliquons ce que cela implique – pour le meilleur et pour le pire – dans notre vie quotidienne. Il est toutefois ironique de constater que plus nous devenons transparents pour les organismes, moins ceux-ci le sont pour nous. Or, l'aspect politique du contrôle des données personnelles requiert que les processus de surveillance soient ouverts, afin que nous puissions en discuter de façon démocratique et que tous jouissent d'un traitement équitable. En somme, nous souhaitons que cet ouvrage encourage les organismes concernés à prendre des mesures afin de mieux rendre des comptes. Dans cette ère numérique, les données, plus particulièrement les données personnelles, sont un enjeu profondément politique.

Remerciements

Le livre est le fruit du travail de nombreuses personnes qui adhèrent au message véhiculé et qui ont fait confiance aux directeurs et à leur assistants pour la publication du produit final. Il a été écrit en collaboration afin d'en maximiser la fiabilité et il a fait l'objet d'une édition collective afin d'en assurer la lisibilité. Les auteurs principaux sont Colin J. Bennett, Andrew Clement, Aaron Doyle, Kevin D. Haggerty, Stéphane Leman-Langlois, David Lyon, David Murakami Wood, Benjamin J. Muller, Laureen Snider et Valerie Steeves. De plus, les professeurs, les boursiers de recherches postdoctorales et les étudiants des cycles supérieurs qui ont contribué à certaines sections du document, dont les annexes, et qui ont proposé des exemples sont Ciara BrackenRoche, Art Cockfield, Alexander Cybulski, Ian McCuaig, Jeffrey Monaghan, Jonathan Obar, Caroline Pelletier, Sachil Singh, et Dan Trottier. Par ailleurs, plusieurs spécialistes de la protection de la vie privée et de la surveillance ont bien voulu poser un regard critique sur le manuscrit : Robin Bayley, Jay Handelman, Peter Hope-Tindall, Philippa Lawson, Pierrot Péladeau, Blaine Price, Chris Prince, Roch Tassé, Micheal Vonn, et Yijun Yu. Les Presses de l'Université d'Athabasca nous ont également offert une aide technique par l'entremise de Pamela MacFarland Holway, Kathy Killoh, Morgan Tunzelmann et Megan Hall. Enfin, la réalisation du projet n'aurait simplement pas été possible sans l'aide d'Anne Linscott et d'Emily Smith pour l'édition et le soutien administratif de Joan Sharpe du Centre des études sur la surveillance de l'Université Queen's. La traduction française du texte a été rendue possible par le travail acharné et la précision de nombreuses personnes, y compris: services de traduction par Amélie Roberge à la Société Gamma Inc, une révision approfondie par Stéphane Leman-Langlois (Université Laval) et Pamela MacFarland Holway à AUP, les commentaires de Mary Jane Knox et révision par Andrée Laprise.

Le programme multidisciplinaire de recherche sur la *Nouvelle transparence : la surveillance et le tri social*, fait partie des Grands travaux de recherche concertée financés par le Conseil de recherches en sciences humaines du Canada (CRSH). Il regroupe plusieurs universités canadiennes ainsi que l'Open University du Royaume-Uni. Cette équipe de recherche se penche sur divers aspects du traitement de l'information personnelle dans le monde numérique d'aujourd'hui (voir www.sscqueens.org/projects/the-new-trans

parency/about/ [en anglais seulement]), mais s'est engagée dès le départ à présenter les résultats de ses enquêtes dans un format accessible pour les Canadiens et les Canadiennes. Nous sommes reconnaissants du soutien continu apporté par le CRSH et nous tenons à remercier toute l'équipe de la Nouvelle transparence et nos partenaires, plus particulièrement le Commissariat à la protection de la vie privée du Canada et la Coalition pour la surveillance internationale des libertés civiles.

Introduction

Comment la vie des Canadiens est-elle devenue transparente ?

Aujourd'hui, nos vies se sont ouvertes aux autres d'une manière sans précédent. Au Canada, comme ailleurs, divers organismes surveillent ce que nous faisons, nous suivent de près, vérifient nos renseignements et suivent nos déplacements. Presque tout ce que nous faisons laisse une trace électronique : nous ne pouvons naviguer sur Internet, marcher au centre-ville, assister à un cours universitaire, payer avec une carte de crédit, monter à bord d'un avion ou faire un appel sans que des données soient capturées. Les renseignements personnels sont recueillis, traités, enregistrés, extraits, achetés, vendus et échangés. Comme jamais auparavant les particuliers, les organismes publics et privés ainsi que les machines ont accès à nos vies, ou plutôt à des traces et des pistes de données, à des fragments de réalité auxquels est réduite notre existence.

Ce phénomène nous inquiète-t-il ? Certains font peu de cas de cette dégradation de la vie privée et la voient comme une conséquence inévitable du monde numérique dans lequel ils vivent. D'autres se disent : « Et alors ? Lorsque les gens vivaient dans des villages ou des petites villes, leur vie était constamment passée au peigne fin. Aujourd'hui, il s'agit seulement d'une nouvelle forme électronique de cette même connaissance publique de la vie privée. » Et d'autres – plus particulièrement ceux qui utilisent les données personnelles pour faire de l'argent – rejettent ces préoccupations en prétextant qu'elles sont mal à propos. À titre d'exemple, déjà en 1999,

Scott McNealy, du géant de l'informatique Sun Microsystems, déclarait que de toute façon, la vie privée n'existe pas et qu'il faudrait s'y faire[1]. Tous se souviendront de la déclaration de Mark Zuckerberg, fondateur de Facebook, en 2010 : « Les gens sont à l'aise, non seulement avec le fait de partager plus d'informations différentes, mais ils sont également plus ouverts, et à plus de personnes. La norme sociale a évolué ces dernières années »[2].

Dans les pages suivantes, nous verrons que ces déclarations sont soit inadéquates, soit fausses. La surveillance nous importe réellement. Elle soulève des questions qui ne se dissiperont pas et qui ne peuvent pas être simplement ignorées. Certes, le phénomène de la surveillance a explosé avec l'avènement de l'ère numérique, mais quels en sont les effets réels ? Le savons-nous ? Il est vrai que les habitants des villages savaient que certains détails de leur vie étaient examinés minutieusement par le reste de la population. Or, aujourd'hui, ce sont les gouvernements et les grandes entreprises, non seulement nos voisins, qui mènent des enquêtes sur nos vies, et ce, à grande échelle. Il est aussi vrai que des systèmes comme ceux de Sun Microsystems visent à amoindrir la vie privée dans certaines circonstances, mais pas de là à ce que la vie privée soit nulle. Selon cette affirmation, les systèmes seraient omniscients et les gens ne peuvent résister ; ce n'est manifestement pas le cas. Bien entendu, les médias sociaux contribuent à repousser les limites de la vie privée, mais la « norme sociale » est beaucoup plus complexe et lourde de conséquences que ce que semble penser M. Zuckerberg. Ces réponses simplistes – et intéressées – à une situation complexe ne tiennent pas compte des conséquences personnelles, sociales et politiques de la surveillance. Comme le dit le gourou canadien de l'Internet, Don Tapscott, « Avec la transparence intégrale, notre identité et nos comportements s'aplanissent et deviennent visibles par tous ; nous perdons le contrôle »[3].

La « Nouvelle transparence » est le titre de ce projet de recherche qui a duré sept ans et qui a mené à la rédaction de cet ouvrage. Ce titre a été choisi pour faire comprendre le fait que *nous nous exposons comme jamais auparavant au regard des tiers*[4]. La quantité de renseignements personnels glanés, traités et conservés de nos jours a atteint un niveau inégalé dans l'histoire de l'humanité. Certains ressentiront sans doute un malaise ou une incertitude quant à leur vie privée en apprenant ce fait. « Je ne voulais pas que cette photo soit vue par un futur employeur », peut-on se rendre compte après coup. « Pourquoi ce magasin me demande-t-il encore mon numéro de téléphone ? » Le sous-titre du projet de recherche est « La surveillance et le tri social ». Ce sous-titre vise à mettre en évidence non seulement notre malaise par rapport au fait

que nous sommes exposés ou plutôt surveillés, mais également une autre question : *Que se passe-t-il lorsque nos renseignements personnels sont recueillis et utilisés par des tiers ?* Il est capital d'avoir le sentiment de contrôler notre image publique, de même que les façons dont nous sommes décrits et catégorisés, puisque cela peut avoir un impact réel sur les possibilités et les choix qui s'offriront à nous. Le traitement que nous recevons varie en fonction de notre profil et modifie notre présent et notre avenir. Il s'agit du tri social.

Le « nous » représente les Canadiens et les Canadiennes. Naturellement, la surveillance transcende les frontières du pays. Cependant, bien qu'un phénomène similaire puisse être observé dans d'autres pays, cet ouvrage braque les projecteurs sur l'augmentation et l'intensification de la surveillance au Canada. Il est faux d'affirmer que les Canadiens ne s'en soucient pas. À titre d'exemple, plus de la moitié (55 %) des Canadiens sondés en 2012 ont indiqué qu'ils s'opposent au fait que les services de police ou du renseignement tirent de l'information du contenu affiché sur les médias sociaux, et ce, même si une ordonnance du tribunal les autorise. De plus, les deux tiers des Canadiens interrogés la même année ont manifesté leur désaccord par rapport à l'énoncé : « Les services de police et les organismes de renseignement devraient avoir plus de pouvoirs en vue de renforcer la sécurité, même si cela signifie que les Canadiens devront renoncer à certaines mesures de protection de leur vie privée »[5]. Enfin, 90 % des répondants s'opposent à ce que des entreprises comme Google vendent de l'information à des tiers[6]. Alors que le phénomène de la surveillance prend de l'expansion, les Canadiens doivent être au courant non seulement des cas précis et étonnants d'atteinte à la vie privée et à la sécurité, mais également des grandes tendances observées en matière de surveillance. Nous avons grand besoin de trouver une façon de mettre en contexte nos expériences, nos inquiétudes et nos attentes au sujet du traitement des données personnelles. Il est également essentiel de faire connaître ces tendances aux décideurs, aux experts techniques, aux agents d'information, aux enseignants et aux autres parties intéressées afin que nous puissions tous contribuer à façonner l'avenir d'un Canada dépendant du numérique.

Qu'est-ce que la surveillance ?

Il n'y a pas si longtemps, le mot *surveillance* évoquait l'image d'agents vêtus d'un trench au col remonté, suivant discrètement des suspects dans des rues

sombres ou cachant des micros dans une maison. De nos jours, ce concept est totalement différent. Nous ne voulons pas dire ici que ce type de surveillance n'est plus utilisé, mais plutôt que ce phénomène est devenu beaucoup plus vaste. Les administrations ont toujours tenu des dossiers et recueilli des renseignements sur les individus à des fins d'efficacité et de renforcement des capacités. Aujourd'hui, grâce aux ordinateurs et aux technologies de communication, ce phénomène a pris encore plus d'ampleur. À titre d'exemple, les classeurs utilisés auparavant pour conserver les documents papier cloisonnaient l'information de manière à ce que peu de personnes y aient accès tandis qu'aujourd'hui, les bases de données consultables sont mises en réseau, ce qui permet de recueillir et de faire circuler l'information d'une façon qui aurait été inconcevable pour les commis de bureau d'autrefois. De plus, aujourd'hui, il est facile d'avoir accès à l'information ; il suffit d'entrer quelques mots clés et en quelques clics, on peut avoir accès à des biographies complètes.

Et cela ne s'arrête pas là. La progression du phénomène ne se limite pas à une augmentation de la circulation des renseignements personnels et à de nouvelles utilisations de l'information pour promouvoir les priorités politiques et économiques actuelles et pour gérer les risques. Au Canada, notamment, nous voyons maintenant notre frontière avec les États-Unis comme un « périmètre de sécurité ». Cette nouvelle conception a eu des conséquences concrètes : les renseignements personnels migrent maintenant plus librement vers le sud ; la protection du commerce international fait maintenant partie intégrante des initiatives de sécurité ; et la gestion du risque détermine maintenant qui est – et qui n'est pas – autorisé à voyager librement au moyen de l'étiquette d'identification par radiofréquence (IRF) dans leur passeport ou par la collecte d'images au moyen de scanneurs corporels.

L'utilisation de l'information personnelle devient alors déterminante ; les gens qui ont un certain type de profil « passent » plus facilement que d'autres. Et, ce principe ne s'applique pas seulement à la frontière, il s'applique également au marché. En effet, votre carte de grand voyageur à l'aéroport et votre carte de fidélité au supermarché ne sont que la pointe de l'iceberg. Si cet iceberg émergeait, on verrait une série de systèmes qui amassent et trient sans arrêt des mines d'information. Voilà pourquoi, à l'aéroport, des Canadiens découvrent qu'ils figurent sur la liste des personnes interdites de vol (appelée « Protection des passagers » au Canada)[7] tandis que d'autres peuvent passer les contrôles de sécurité les yeux fermés. Et pourquoi lorsqu'ils parlent avec un responsable du service à la clientèle,

certains se voient récompenser de façon inattendue et d'autres ne peuvent aller au-delà du message automatisé « votre appel est important pour nous ». La surveillance est à la base de tous ces processus.

De nos jours, la surveillance ne consiste pas seulement à suivre la trace des « mauvaises » personnes ou des individus « dangereux ». Conjugués, les statistiques et les logiciels ont transformé la surveillance en une manière de classer les gens en fonction des données personnelles disponibles. Alors qu'auparavant, on ciblait des personnes, aujourd'hui, on cible des profils. Et, comme nous l'avons vu, ce profil a un impact important. Vous aurez tôt fait de savoir si le profil qui vous est associé vous classe dans la catégorie des gens à risque ou des gens fiables, des gens à récompenser ou des gens à rabrouer. Comment en sommes-nous arrivés là ? Quelle information pousse notre profil dans une direction et non dans l'autre ? Auparavant, la surveillance consistait à « épier » ; elle consiste aujourd'hui à « observer au moyen de données ». La manière dont ces données sont recueillies, manipulées et utilisées est donc cruciale.

« Qu'est-ce que la surveillance ? » Nous la définissons comme *tout intérêt particulier accordé systématiquement à de l'information personnelle en vue d'influencer, de gérer, d'autoriser ou de contrôler les personnes à qui se rapportent les renseignements amassés*. Présentée de cette façon, il est évident que la surveillance peut être une bonne ou une mauvaise chose, qu'elle peut être acceptable ou non. Il est également évident que la surveillance est plus que le simple fait d'observer, d'espionner ou d'écouter clandestinement les autres. La surveillance est une pratique organisationnelle répandue, qui entraîne souvent une catégorisation des gens de manière à faciliter l'application d'un traitement différent à différentes personnes. De Google au Homeland Security des États-Unis, en passant par l'Agence du revenu du Canada et la Gendarmerie royale du Canada, ce type de surveillance est primordial. Nous devrions peut-être dire ce *triage* de la surveillance, car la grande question est : « Comment sommes-nous triés socialement par la surveillance d'aujourd'hui ? ».

Par ailleurs, l'expansion rapide de plusieurs types de surveillance a fait émerger ou a permis une croissance dans de nouveaux segments[8]. Cet ouvrage porte surtout sur la surveillance effectuée par les *organismes* qui recueillent des données sur les personnes et la population et qui établissent des profils à diverses fins. Or, les particuliers procèdent de plus en plus à de la surveillance à petite échelle. Ils installent un système de sécurité à domicile, cachent une caméra dans un ours en peluche ou une horloge pour surveiller la gardienne, ou suivent les autres au moyen des médias sociaux (se reporter à la neuvième

tendance). D'autres pourraient tenter de rendre la pareille aux organismes en repérant les pratiques organisationnelles abusives ou illégales. Cependant, la différence fondamentale entre les particuliers et les organismes réside dans le type de pouvoirs qu'ils peuvent exercer. Bien que les simples utilisateurs de Facebook aient accès au plus important système de reconnaissance faciale du monde (la fonction « identifier » de la plateforme), ils ne contrôlent pas les algorithmes qui permettent de classer les gens par groupes auxquels s'appliquent différents traitements. Voilà pourquoi la dimension du tri social qui relève essentiellement des grands organismes est indispensable pour comprendre la surveillance actuelle.

La surveillance est devenue un phénomène omniprésent et complexe. D'une part, il ne s'agit que de la façon de faire normale de bon nombre d'organismes et elle n'a souvent pas de conséquences graves. D'autre part, il s'agit d'une forme de pouvoir qui touche tout le monde, parfois en tant que personne identifiable et parfois en tant que population. Certains groupes sont plus visés par la surveillance que d'autres. Néanmoins, dans tous les cas, l'équilibre des pouvoirs entre les particuliers et les organismes change en raison du nombre croissant de nouvelles pratiques et de nouveaux processus de surveillance. Alors, bien que la surveillance puisse donner de bons ou de mauvais résultats, elle n'est jamais neutre. De plus, les enjeux sont beaucoup trop importants pour s'en remettre aux employés de bureau, aux politiciens ou aux experts techniques. Dans cet ouvrage, nous mettrons l'accent sur les facettes douteuses de la surveillance et nous conclurons en proposant des moyens de relever le défi auquel nous faisons face.

La surveillance au Canada : le contexte

Comme dans tous les autres pays, la surveillance est essentielle au gouvernement et au commerce au Canada. En effet, dès les années 1960 le Canada montre un intérêt précoce pour la haute technologie et la croissance de l'infrastructure de l'information. À cette époque, le Canada devient un chef de file du traitement des renseignements personnels, à l'aide du recours hâtif aux ordinateurs centraux et de l'installation du réseau téléphonique pancanadien. L'efficacité des opérations était considérée comme un objectif clé. Des valeurs socio-politiques ont toutefois toujours influencé la façon dont l'informatisation se déroulait et son incidence sur différents groupes[9]. Par exemple, dès 1940, le Bureau fédéral de la statistique (le prédécesseur de

Statistique Canada) utilisait des cartes à perforer, des trieuses et des tabulatrices dans le cadre du programme de conscription dans les forces armées. Les Allemands, les Italiens, les Japonais et les Doukhobors en étaient exclus, de même que les résidents chinois et indiens[10]. Cependant, le tri social a augmenté et s'est accentué depuis. Aujourd'hui, la technologie de l'information (TI) permet une classification plus précise des groupes, augmente la dépendance vis-à-vis des entreprises privées ainsi que facilite et favorise le partage de renseignement au sein des organismes et entre ceux-ci[11].

Nous devons toutefois mentionner que la nécessité d'imposer des limites légales au traitement de l'information a été admise dès le départ. Voilà pourquoi le Canada est considéré dans le monde entier comme un modèle de protection des données personnelles et de respect de la vie privée. Le réseau canadien de commissaires à la protection de la vie privée, qui peuvent recevoir des plaintes et y donner suite, fait l'envie de nombreux pays. D'ailleurs, les Canadiens peuvent être reconnaissants à bien des égards puisque le gouvernement s'est engagé à protéger les simples citoyens des risques et des dangers liés à la circulation des données personnelles. Au cours des dernières décennies, des progrès considérables ont été accomplis.

À titre d'exemple, des dispositions sur la protection des données ont été adoptées dans la *Loi canadienne sur les droits de la personne* en 1977 ; la *Charte canadienne des droits et libertés* (1982) comprend une « protection contre les fouilles, les perquisitions ou les saisies abusives » dont l'interprétation inclut la protection de la vie privée ; et la *Charte des droits et libertés de la personne du Québec* (article 5, 1976) stipule que « toute personne a droit au respect de sa vie privée ». La première *Loi sur la protection des renseignements personnels* a été adoptée en 1983 au Canada et réglementait l'utilisation, la collecte et la divulgation de renseignements personnels par le gouvernement fédéral. En 2000, le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques*, pour régir l'utilisation des données personnelles dans un contexte commercial. Cette *Loi* est entrée en vigueur en 2004.

À l'opposé, d'autres pays ont tardé à prendre des mesures ou ont édicté des mesures de protection plus faibles. À titre d'exemple, bien que les États-Unis aient adopté en 1974 une loi sur la protection des renseignements personnels, soit avant le Canada, ils n'ont pas instauré d'entité comme le Commissariat à la protection de la vie privée du Canada. Le Commissariat fédéral a été créé en 1977 pour superviser et surveiller la conformité à la loi sur la protection de la vie privée. Les Américains sont ainsi renvoyés aux

tribunaux pour les plaintes ou les accusations découlant des dispositions législatives sur la vie privée. De plus, l'Ontario a été la première province à créer en 1988 le Bureau du commissaire à l'information et à la protection de la vie privée. Cet organe supervise le respect de la vie privée et l'accès à l'information. Il faut admettre que certains estiment que ce mandat est contradictoire et qu'il affaiblit l'influence du commissaire. Au fédéral, une importante disposition rendant le consentement obligatoire figure dans la *Loi de 2000 sur la protection des renseignements personnels et les documents électroniques*. Conformément à cette disposition, les organismes doivent obtenir le consentement de la personne concernée pour recueillir, utiliser ou divulguer ses renseignements personnels.

Le Canada ne peut toutefois pas se reposer sur ses lauriers. La technologie évolue rapidement, tout comme les pratiques commerciales et gouvernementales. Si l'on pense à la sécurité nationale et surtout aux médias sociaux, les problèmes liés à la manipulation des données personnelles se sont multipliés à un rythme fulgurant depuis 2000. Aujourd'hui, la sécurité dans les aéroports comprend des procédures de collecte de données et d'établissement de profils – prise d'empreintes, surveillance par caméra, intégration de composantes électroniques dans les passeports – que l'on n'aurait pu imaginer à la fin des années 1990. Par ailleurs, qui aurait cru que les données personnelles seraient partagées avec autant de liberté – ou de façon aussi imprudente selon certains – sur les médias sociaux ? Qui aurait cru qu'une entreprise comme Facebook puisse faire des profits en vendant les données personnelles de ses utilisateurs et ferait de son propriétaire le plus jeune milliardaire de la planète en seulement quelques années.

Cependant, si nous considérons ce que le simple Canadien en pense, il y a lieu de s'inquiéter. Plus des deux tiers des Canadiens interrogés en 2006 puis en 2012 par Vision Critical ont indiqué qu'ils se préoccupent de leurs données personnelles et qu'ils prennent également des mesures pour se protéger, notamment en lisant les politiques de protection de la vie privée lorsqu'ils font un achat auprès d'une entreprise privée et en refusant de donner de l'information aux entreprises lorsqu'ils ne croient pas qu'il est nécessaire de le faire. Par ailleurs, lors du sondage de 2012, ce pourcentage s'est élevé à 79 %[12]. Les Canadiens sont bien conscients que ces enjeux les touchent.

De plus, plus de la moitié des Canadiens s'en remettent simplement au gouvernement pour s'occuper adéquatement de leurs données personnelles. Par contre, selon un sondage de Vision Critical qui a fait date en 2006, moins

de la moitié de la population sait qu'il existe des lois pour protéger les renseignements personnels (ce pourcentage s'est abaissé de 8 % selon un sondage de suivi mené en 2012)[13]. Seulement un tiers des Canadiens pensent qu'ils peuvent exercer une forme de contrôle quant à l'utilisation de leurs données. Presque tous les Canadiens font état d'inquiétudes quant à la sécurité des données détenues par le gouvernement et pensent qu'il est possible que ces données se retrouvent entre les mains du secteur privé (un peu moins de la moitié des Canadiens interrogés font confiance aux entreprises pour la protection de leurs données) ou de gouvernements étrangers (comme cela se produira conformément aux nouvelles dispositions frontalières relatives au périmètre de sécurité qui augmentent l'échange de données personnelles avec les États-Unis). Les Canadiens sont également méfiants lorsqu'il est question de sécurité nationale. Plus de la moitié des répondants ont indiqué que les mesures de sécurité nationale portent atteinte à la vie privée (ce chiffre est demeuré le même en 2012) ; nombre d'entre eux croient que le gouvernement ne devrait pas partager de renseignements personnels avec la police sauf si une personne est soupçonnée d'un acte répréhensible. Près de 37 % des Canadiens sont convaincus que les minorités visibles ne devraient pas subir de contrôles de sécurité additionnels ; ce pourcentage a toutefois diminué en 2012[14].

Dans ce contexte, il existe des différences subtiles et parfois moins subtiles entre le Québec et le reste du Canada. Selon le sondage de 2006 cité précédemment, les Québécois se montrent dans l'ensemble plus optimistes quant aux avantages de la surveillance et moins préoccupés par la collecte et l'utilisation de leurs renseignements personnels que les résidents des autres provinces du Canada. Moins de Québécois s'inquiètent, notamment, de l'avènement possible d'une carte d'identité nationale et un pourcentage moins élevé croit que les mesures de surveillance pour la sécurité nationale ne respectent pas la vie privée. À cet égard, ils ont parfois des vues plus similaires aux résidents des pays d'Europe, dont bon nombre ne semblent pas être aussi alarmés par la montée de la surveillance.

Cependant, si les résultats des sondages sur la surveillance et la protection de la vie privée nous indiquent quelque chose, c'est bien que les Canadiens se soucient d'enjeux comme celui de l'établissement de profils. En effet, plus de la moitié des Canadiens interrogés en 2006 et en 2012 s'opposent notamment à ce que les minorités visibles soient ciblées dans les aéroports. Or, lorsqu'il est question des récompenses offertes par les programmes de fidélisation ou de la vente de profil personnel de marketing, plus de la moitié

des Canadiens estiment que ce type de tri social est acceptable. Il est néanmoins difficile pour les enquêteurs de cerner les conséquences *négatives* sur les particuliers que peut avoir l'établissement de profils par les responsables-marketing[15]. Peu de citoyens comprennent réellement la marginalisation dont sont victimes certaines personnes dans plusieurs sphères de leur vie ; les désavantages s'accumulent d'une façon disproportionnée pour les catégories de personnes rejetées par les annonceurs, les responsables-marketing et les fournisseurs de service[16].

La surveillance au Canada : les facteurs

Une partie du problème réside dans le fait que les gouvernements et les entreprises construisent des infrastructures de surveillance à une vitesse telle que le public n'a pas le temps de se renseigner et de discuter des conséquences. Pourquoi la surveillance connaît-elle une croissance si rapide ? Qu'est-ce qui motive la surveillance ou qu'est-ce qui lui permet de s'immiscer dans tous les aspects imaginables et inimaginables de nos vies ? La technologie, les lois, la politique, l'économie, la culture ainsi que nos propres perceptions et nos pratiques jouent toutes un rôle. L'expansion rapide de la surveillance au Canada n'est pas motivée par un seul facteur. Combinées, les pressions exercées à plusieurs égards et par bon nombre de sources ont toutefois catapulté la chasse aux renseignements personnels. Or, une partie de cette expansion semble relativement inoffensive tandis que d'autres aspects semblent franchement nuisibles. Ccertains éléments font partie d'une politique délibérée tandis que d'autres sont une conséquence non intentionnelle d'un processus légitime ou même souhaité. Nous aborderons ces éléments, mais commencerons par donner un aperçu de certaines des causes sous-jacentes à l'amplification de la surveillance au Canada.

Le premier facteur est le *potentiel technologique.* Au cours des dernières décennies, on a mis au point des outils qui facilitent grandement la surveillance systémique. Une croyance répandue dans notre culture, en particulier en Amérique du Nord, veut que la technologie soit une solution clé aux problèmes sociaux et politiques[17]. Ainsi, l'adoption de nouveaux outils de gestion de haute technologie conduit souvent à des solutions de surveillance. On peut faire la démonstration de cette foi en la technologie de la façon suivante : même si des solutions non technologiques existent et que les solutions technologiques ne fonctionnent pas nécessairement comme on

le prétend, la rapidité à laquelle les nouvelles technologies sont adoptées et déployées demeure toujours aussi intense.

Ce premier facteur est étroitement lié au deuxième : *l'économie des renseignements personnels*[18]. Les données personnelles sont une mine d'or pour les entreprises. Prenons l'exemple de Facebook dont la valeur, dès son introduction en Bourse en 2012, était estimée à 104 milliards de dollars. De plus, les données personnelles présentent une valeur très élevée pour les ministères ainsi que pour les services de police, les agences du renseignement et les services de sécurité. D'ailleurs, les renseignements personnels sont souvent appelés le « pétrole » du XXIe siècle[19] ; il pourrait donc être utile de réfléchir aux risques qui y sont associés ! Il y a plus de 20 ans, les consommateurs se sont révoltés lorsque Lotus Corporation a lancé Household Marketplace, un logiciel qui aurait permis d'enregistrer le nom, l'adresse, les revenus et le nombre d'enfants de chaque ménage aux États-Unis[20]. Aujourd'hui, ce genre d'activités parallèles est banal. En 2006, la Clinique d'intérêt public et de politique d'internet du Canada a produit un rapport sur les « courtiers en données » au Canada. Dans ce rapport, la Clinique illustre comment des renseignements détaillés sur les particuliers se retrouvent entre les mains d'organismes avec qui ils n'ont aucun lien. Elle explique que les courtiers peuvent vendre de l'information aux entreprises et aux gouvernements. Enfin, les auteurs du rapport ont conclu que l'accumulation croissante des données personnelles et le regroupement des bases de données rendaient les individus vulnérables aux abus que pourraient commettre les personnes ayant accès à ces données[21].

Le troisième facteur est le virage vers le *néolibéralisme,* c'est-à-dire l'adoption de politiques gouvernementales qui mettent l'accent sur le libre-échange et la déréglementation des marchés. Dans sa forme actuelle, le néolibéralisme favorise les activités économiques du secteur privé par rapport à celles du secteur public. De ce point de vue, c'est le marché qui doit assurer la prospérité de tous et l'État doit se limiter à des fonctions militaires et politiques, soit l'ordre public et la sécurité. L'exemple de Lockheed Martin illustre très bien ce virage : l'entreprise mène pour le gouvernement du Canada des activités relatives au soutien des TI et à l'armement. Les accords de libre-échange entre le Canada et les États-Unis encouragent ce genre d'interaction économique. Parallèlement, un renforcement de la fonction de sécurité se traduit par des profits pour les entreprises canadiennes. Cependant, l'état libéral est parfois loin d'être libéral dans la façon dont il s'efforce de modeler l'avis, les attentes et les choix de la population au moyen

de la surveillance. Il arrive parfois notamment qu'une manifestation légitime soit considérée comme un acte séditieux, voire terroriste. Prenons par exemple la description que fait le Centre intégré d'évaluation du terrorisme des activités de certains groupes environnementalistes[22].

Le quatrième facteur est étroitement lié au néolibéralisme et concerne la priorité généralement accordée à la *gestion des risques.* Depuis des décennies, et plus particulièrement depuis les années 1980, le Canada s'appuie largement sur l'analyse des risques pour orienter les politiques publiques. Comme beaucoup d'incertitudes entourent la vie normale – des accidents aux catastrophes en passant par les échecs financiers et l'effondrement des projets – les gouvernements et les entreprises qui y sont associées ont besoin d'outils pour atténuer ou réduire au minimum les risques tout en maximisant les possibilités. Or, pour déterminer quels sont les risques, de l'information est nécessaire. C'est là où la surveillance entre en jeu. Selon une étude sur la politique canadienne qui a fait date, le maintien de l'ordre a été transformé à la fin du XXe siècle par les nouvelles technologies conçues pour déterminer et faire le suivi des risques. Pour accomplir cette tâche, les policiers utilisent la surveillance pour observer les gens puis les catégoriser selon le niveau de risque qu'ils pourraient présenter[23]. Une fois de plus, le tri social constitue le revers de la surveillance. Il est donc plus difficile pour une personne classée dans la catégorie des « mauvais » de prouver son innocence puisque la présomption de culpabilité est la position adoptée par défaut jusqu'à ce que le système prouve le contraire.

Cette grande orientation nous mène au cinquième facteur : la *sécurité nationale.* Les organismes responsables de ce dossier avaient déjà pris de l'expansion au XXe siècle, mais les attaques du 11 septembre leur ont donné un formidable coup d'accélérateur. La logique de la gestion du risque s'applique aussi ici. Les voyageurs le savent très bien ; pour répondre aux exigences de sécurité nationale, ils doivent maintenant enlever leurs chaussures, jeter les liquides et ouvrir leur ordinateur portable. Toutefois, ces mesures de sécurité comprennent de plus en plus une vérification corporelle et une inspection des bagages. Avez-vous déjà remarqué le nombre de caméras fixées au plafond lorsque vous passez les contrôles de sécurité à l'aéroport ? L'Administration canadienne de la sûreté du transport aérien est responsable de ces caméras, de même que du maintenant célèbre scanneur corporel. Fait plus important encore, bien avant le départ, les données des passagers sont utilisées pour suivre leurs déplacements. Par ailleurs, le facteur « sécurité nationale » s'étend à la fois bien au-delà et bien en deça de ce qui est « national ». D'une

part, il prend appui sur un réseau de pays participants qui dépasse de plus en plus le contrôle du gouvernement du Canada (se reporter à la Tendance 6). D'autre part, il justifie également l'avènement de la vigilance dans beaucoup d'autres domaines ; on considère maintenant que les lieux publics, les complexes sportifs et les écoles ont une dimension de « sécurité ».

Le sixième facteur est la *perception du public,* laquelle permet ou prescrit les avancées dans le domaine de la surveillance. Bien qu'il soit clair, comme nous l'avons mentionné auparavant, qu'une bonne partie des Canadiens font preuve de prudence, voire sont négatifs, quant à la vaste portée de la surveillance – rappelons que 60 % des Canadiens estiment que la surveillance à des fins de sécurité constitue une atteinte à la vie privée – d'autres acceptent avec réticence ou résignation une vigilance qui va croissant. Cette donnée est importante ; il est plus facile de prendre de nouvelles mesures de surveillance, si on rend les gens enclins à les accepter. Le climat de peur qui caractérise la vie au Canada, particulièrement depuis le 11 septembre, pousse nombre de personnes à accepter une plus grande surveillance[24]. À cela, il faut ajouter que notre accoutumance à la surveillance commerciale en ligne rend la surveillance dans d'autres domaines plus facile à accepter[25]. Par ailleurs, lorsque les citoyens n'aiment pas les nouvelles mesures adoptées, les autorités en prennent note. À titre d'exemple, citons la pétition en ligne signée par un nombre sans précédent de citoyens, soit 145 000, pour protester contre les dispositions du projet de loi C-30 sur « l'accès légal », selon lesquelles les services de police auraient pu obliger sans mandat les fournisseurs de services Internet et d'autres à fournir des données sur leurs abonnés[26].

Le septième facteur est l'adoption de *nouvelles lois* qui permettent ou requièrent la surveillance ou qui assouplissent les limites légales de la surveillance. On exerce notamment des pressions de plus en plus grandes pour que des exemptions aux dispositions sur la protection des renseignements personnels soient admises. Les dispositions sur « l'accès légal » du projet de loi C-30 en sont un exemple flagrant. D'ailleurs, la commissaire à l'information et à la protection de la vie privée de l'Ontario, Mme Ann Cavoukian, a indiqué que le projet de loi constituait l'une des menaces les plus envahissantes à notre vie privée et à notre liberté qu'elle ait vue[27]. Or, des menaces semblables peuvent émaner des lois actuelles. À titre d'exemple, si un organisme peut prouver qu'il se conforme aux principes élémentaires de la protection des renseignements personnels, il peut légalement procéder à la surveillance, et ce, en toute impunité. Lancé en 1997, le programme nommé Projet de remaniement des activités a comme objectif de réduire le nombre

de fraudes relatives à l'aide sociale en Ontario. Pour ce faire, on a recours à plusieurs outils de surveillance comme le Processus de vérification détaillée qui permet de vérifier le droit à l'aide sociale tous les 12 mois. Cet outil permet de diminuer le temps que les agents de traitement des cas consacrent à leurs clients à faible revenu et d'augmenter le nombre de justifications que doivent fournir ces clients pour leurs activités quotidiennes. Personne ne suggère que les responsables de l'aide sociale en Ontario contreviennent aux lois sur la protection des renseignements personnels lorsqu'ils fournissent de l'information à d'autres organismes gouvernementaux. Cependant, on a établi que de la discrimination négative était bel et bien entraînée par leurs activités, surtout à l'égard des mères célibataires[28].

La surveillance au Canada : les tendances

La meilleure façon de saisir l'ampleur des changements en matière de surveillance qui touchent les Canadiens est de se pencher sur les tendances générales observées. Dans cet ouvrage, nous analyserons neuf grandes tendances, des changements à grande échelle qui s'opèrent à un rythme jamais vu auparavant. En réalité, dans les circonstances actuelles, il est difficile de se rappeler quel était l'état de la situation avant le 11 septembre ou avant l'arrivée des médias sociaux. L'histoire de la surveillance, dans son ensemble, peut être racontée comme une transformation d'avant à après. Jadis, Lotus Corporation (cella-là même qui tenta de lancer un système de suivi des noms, des adresses, des niveaux de revenus et du nombre d'enfants de chaque ménage aux États-Unis) fut contrainte de faire marche arrière lorsque les consommateurs s'opposèrent à ce projet digne du roman de George Orwell. Aujourd'hui, avec un seul clic de souris, les utilisateurs des médias sociaux divulguent bien plus de renseignements intimes à un large éventail d'entreprises. Auparavant, une personne pouvait passer la frontière canado-américaine avec un permis de conduire. Aujourd'hui, les données personnelles de cette personne sont scrutées à la loupe et arrivent à la frontière avant elle. De plus, cette personne doit présenter un permis de conduire Plus ou un passeport aux agents d'immigration. Et ainsi de suite. Chacune des tendances étudiées dans cet ouvrage sert à expliquer l'interaction entre les différentes influences qui amplifient le phénomène de la surveillance. De plus, chacune de ces tendances a une incidence profonde sur la vie sociale, la liberté et la justice dans le Canada du XXIe siècle.

La première tendance, l'*expansion de la surveillance,* rend compte de certaines dimensions de l'intensification de la surveillance et montre que les pratiques qui jadis étaient considérées comme une nouveauté sont maintenant considérées comme une normalité. La deuxième tendance, la *sécurisation et surveillance*, est assimilée au facteur de la « sécurité » : un nombre croissant de sphères de la vie sont considérées comme à risque et nécessitent donc d'être surveillées pour en assurer la sécurité. L'identité de ceux qui effectuent cette surveillance, toutefois, est de moins en moins claire puisque des organismes publics et privés jouent chacun un rôle qui est tantôt complémentaire, tantôt interactif. C'est ce qu'illustre la troisième tendance, le *décloisonnement des secteurs*. Ce décloisonnement caractérise également la quatrième tendance, l'*ambiguïté croissante des renseignements personnels*. Il est de moins en moins facile de déterminer quelles sont les données qui permettent d'identifier une personne, mais il est de plus en plus clair que la surveillance augmente malgré les ambiguïtés.

Chose certaine, la surveillance ne vise plus seulement à savoir qui vous êtes et ce que vous faites, mais également à savoir *où* vous êtes. La cinquième tendance est l'*augmentation de la surveillance mobile et de la géolocalisation*. Ces types de surveillance se retrouvent dans différentes régions du monde ; ainsi, la sixième tendance est la *mondialisation de la surveillance*. Cette tendance est complexe puisqu'en raison de leur culture et de la situation locale, les gens vivent la surveillance de façon différente. À titre d'exemple, la surveillance au Canada est fortement influencée par les tendances mondiales, mais on y applique le filtre des lois, des traditions et des cultures canadiennes. La septième tendance, l'*intégration de la surveillance dans des contextes quotidiens,* montre que la surveillance tend vers l'omniprésence, intégrée à une foule d'objets, notamment aux voitures, aux immeubles et aux maisons. Or, cette omniprésence ne se limite pas aux objets : la *surveillance vise de plus en plus le corps*. Cette huitième tendance traduit la façon dont notre corps est utilisé au quotidien comme une source de données. Nos empreintes digitales, notre ADN et notre démarche n'en sont que quelques exemples.

La neuvième tendance, la *surveillance sociale croissante*, est en quelque sorte la plus récente, mais, elle s'est révélée, sans conteste, extrêmement importante. Bien que le fait qu'une personne en observe une autre n'ait rien de nouveau, les médias sociaux ont entraîné une explosion de ce phénomène. Parmi les tendances, cette dernière est extraordinaire. Des inquiétudes d'après-guerre au sujet de *Big Brother*, ce tyran excessivement vigilant, à la domestication de la surveillance par le marketing, dont les responsables

scrutent les données des consommateurs, nous bouclons la boucle en nous surveillant les uns les autres. Bien entendu, ce type de surveillance a bien peu d'importance si on le compare à ce que peuvent faire Google ou le Service canadien du renseignement de sécurité (SCRS). Néanmoins, le fait de faire nous-mêmes de la surveillance à petite échelle rendrait-il plus acceptables et normaux les autres types de surveillance ?

Quelles solutions s'offrent donc à nous ?

Les tendances décrites dans l'ouvrage *Vivre à nu : la surveillance au Canada* brossent un portrait saisissant. Ensemble, elles montrent que, bien que plusieurs formes de surveillance aient des résultats positifs, au fur et à mesure que la surveillance augmente, le rapport de force entre les individus et les organismes tend à pencher dangereusement vers les organismes. Alors, pouvons-nous avoir confiance en ces autorités, gouvernements ou entreprises qui nous surveillent constamment ? À quel point sont-ils tenus de rendre des comptes quant à nos données personnelles ? Dans cet ouvrage, nous allons au-delà de l'analyse des tendances et en tirons des conclusions. Nous formulons également des réponses stratégiques ainsi que des recommandations particulières. Par-dessus tout, nous souhaitons susciter le débat public impératif qui doit être tenu à plusieurs chapitres.

Notes

1 Voir Polly Sprenger, « Sun on Privacy: 'Get Over It' », *Wired,* 26 janvier 1999, http://www.wired.com/politics/law/news/1999/01/17538.

2 Voir l'entrevue avec Zuckerberg de Marshall Kirkpatrick, « Facebook's Zuckerberg Says the Age of Privacy Is Over », *ReadWrite*, 9 janvier 2010, http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php.

3 Don Tapscott, « Is Privacy an Outmoded Idea in the Digital Age ? », *Toronto Star*, 1er juin 2012, http://www.thestar.com/news/insight/article/1204668--don-tapscott-on-privacy-in-a-digital-ageis-privacy-in-the-digital-age-an-outmoded-idea/.

4 Pour en savoir plus sur le projet de recherche sur la Nouvelle transparence, consultez le http://www.sscqueens.org/projects/the-new-transparency *(en anglais seulement)*.

5 Frank Graves, *An Increasingly Divided Outlook: Rethinking Canada's Place in the World*, exposé au symposium Walter Gordon 2012 sur la politique publique, École de politiques publiques et de gouvernance, Université de Toronto, 20 mars 2012, http://www.ekospolitics.com/wp-content/uploads/2012_walter_gordon_symposium_presentation.pdf.

6 The Globalization of Personal Data Project, International Survey on Privacy and Surveillance, http://qspace.library.queensu.ca/handle/1974/7656. Voir aussi *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons,* publié sous la direction de Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon et Yolande E. Chan (Montréal et Kingston, McGill-Queen's University Press, 2010).

7 Canada, Sécurité publique, *Protéger les Canadiens grâce au Programme de protection des passagers*, 2013, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/index-fra.aspx.

8 Voir la présentation des divers types de surveillance dans Charles Raab et Colin J. Bennett, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA, MIT Press, 2006), p. 23-26.

9 Voir, par exemple, Michael Adler et Paul Henman, « Computerizing the Welfare State », *Information, Communication and Society* 8, nº 3 (2005), p. 315-342.

10 Voir Scott Thompson, *Consequences of Categorization: National Registration, Surveillance and Social Control in Wartime Canada, 1939-1946*, thèse de doctorat, Université de l'Alberta, 2013.

11 Kenneth Kernaghan et Justin Gunraj, « Integrating Information Technology into Public Administration », *Canadian Public Administration/Administration Publique du Canada* 47, nº 4 (2004), p. 525-546.

12 Vision Critical est une subsidiaire de la compagnie Angus Reid Global, basée à Vancouver. Pour consulter les statistiques de 2006, voyez « The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance --Summary of Findings, November 2008 », http://qspace.library.queensu.ca/bitstream/1974/7660/1/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf, 14 -15. Aussi, « The Globalization of Personal Data (GPD) Project, International Survey on Privacy and Surveillance », http://qspace.library.queensu.ca/handle/1974/7656. Enfin, on peut consulter une analyse des résultats internationaux du sondage de 2006 dans Zureik *et al.*, (dir.) Surveillance, Privacy, and the Globalization of Personal Information. Pour ce qui est des statistiques de 2012, on peut les trouver chez Angus Reid Global dans « Privacy and Surveillance: June 2012 Globalization of Personal Data Follow-Up » (Vancouver: Angus Reid Global, 2012), http://qspace.library.queensu.ca/handle/1974/8623, table 71. Ce rapport est mis à disponibilité grâce au Data and Government Information Centre de l'Université Queen's. Les tableaux peuvent être téléchargés à l'aide du URL fourni.

13 « The Globalization of Personal Data Project », p. 11; Angus Reid Global, « Privacy and Surveillance », tableau no. 29.

14 « The Globalization of Personal Data Project », pp. 13, 26, et 33; Angus Reid Global, « Privacy and Surveillance », tableaux no. 33 et 44.

15 « The Globalization of Personal Data Project », p. 33–34; Angus Reid Global, « Privacy and Surveillance », tableau no. 44.

16 Voir Oscar Gandy, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage* (Farnham, Royaume-Uni, Ashgate, 2009) ; et Joseph Turow, *The Daily You: How the Advertising Industry Is Defining Your Identity and Your Worth* (New Haven, Yale University Press, 2012).

17 Pour la croyance sur l'efficacité de la technologie, voir par exemple Vincent Mosco, *The Technological Sublime* (Cambridge, MA, MIT Press, 2004) ; et Arthur Kroker, *Technology and the Canadian Mind* (Montréal, New World Perspectives, 1984).

18 On ne sait pas exactement qui a inventé cette expression, mais elle est utilisée notamment par Perri 6, dans le chapitre « The Personal Information Economy: Trends and Prospects for Consumers » de *The Glass Consumer: Life in a Surveillance Society,* publié sous la direction de

Susanne Lace (Bristol, Royaume-Uni, Policy Press, 2005), et par Greg Elmer, dans *Profiling Machines; Mapping the Personal Information Economy* (Cambridge, MA, MIT Press, 2004).

19 Voir, par exemple, Mike Klein, « Major Trends for Enterprise IT: Information Will Be Oil of 21st Century, Gartner Says », *WTN News*, 19 octobre 2010, http://wtnnews.com/articles/7897/.

20 Voir Denise Caruso, « Digital Commerce: Personal Information Is Like Gold in the Internet Economy », *New York Times,* 1er mars 1999, http://www.nytimes.com/1999/03/01/business/technology-digital-commerce-personal-information-like-gold-internet-economy-rush.html.

21 Voir Canadian Internet Policy and Public Interest Clinic, *On the Data Trail: How Detailed Information About You Gets into the Hands of Organizations with Whom You Have No Relationship—a Report on the Canadian Data Brokerage Industry,* Ottawa, 2006, www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf.

22 Voir Carys Mills, « Terrorism Monitor Closely Watched Occupy Protests », *Globe and Mail*, 10 avril 2012, http://www.theglobeandmail.com/news/national/terrorism-monitor-closely-watched-occupy-protests/article4098990/. Pour une analyse plus vaste, voir le texte de Didier Bigo, « Security, Surveillance and Democracy », dans Kirstie Ball, David Lyon et Kevin Haggerty (dir.), *The Routledge Handbook of Surveillance Studies* (Londres et New York, Routledge, 2012), p. 277-284 ; et de David Garland, *The Culture of Control* (Chicago, University of Chicago Press, 2001).

23 Richard Ericson et Kevin Haggerty, *Policing the Risk Society* (Toronto, University of Toronto Press, 1997), p. 449.

24 Voir, par exemple, David Lyon, *Surveillance After September 11* (Cambridge, Royaume-Uni, Polity Press, 2003).

25 Le sondage mené en 2012 par Vision Critical montre que près de 50 % des personnes interrogées, qu'elles utilisent ou non les médias sociaux, étaient d'accord pour que les employeurs puissent avoir recours aux médias sociaux pour faire des vérifications sur les employés (The Globalization of Personal Data Project, International Survey on Privacy and Surveillance, http://qspace.library.queensu.ca/handle/1974/7656). Une telle acceptation de la surveillance témoignerait-elle du fait que des attitudes similaires seraient également observées dans d'autres domaines comme la surveillance pour la sécurité nationale ?

26 Voir Laura Payton, « Online Surveillance Bill Opponents Continue Campaign », *CBC News*, 24 mai 2012, http://www.cbc.ca/news/politics/story/2012/05/24/pol-lawful-access-c-30-campaign.html.

27 Ann Cavoukian, *Toujours vigilants*, Rapport annuel 2011 du Commissaire à l'information et à la protection de la vie privée de l'Ontario, Toronto, http://www.ipc.on.ca/french/resources/annual-reports/annual-reports-summary/default.aspx?id=1193.

28 Voir, par exemple, Krystle Maki, « Neoliberal Deviants and Surveillance: Welfare Recipients Under the Watchful Eye of Ontario Works », *Surveillance and Society* 9, nº 1 (2011), p. 47-63.



Augmentation de la surveillance

De l'exception à la routine

La surveillance fait constamment la une. Elle soulève certaines des questions sociales, politiques et éthiques qui sont impératives de nos jours. En même temps, elle n'est pas une nouveauté. La surveillance interpersonnelle face à face est une caractéristique inhérente à la coexistence entre les humaines et les organismes utilisent depuis longtemps la surveillance à différentes fins[1]. Cependant, l'expansion, l'intensification et l'intégration des mesures de surveillance en sont arrivées à un tournant historique[2]. Nous devons simplement faire face à plus de surveillance aujourd'hui et les systèmes de surveillance que nous utilisons sont dotés de capacités jamais vues. Ces capacités permettent de voir plus, d'aller plus loin et de créer plus de nouveaux liens qu'il était possible de le faire auparavant. Cette expansion et cette intensification sont peut-être les changements les plus remarquables et les plus inquiétants de la dynamique de la surveillance et de la vigilance.

Nous prendrons les exemples de deux cadres institutionnels différents pour illustrer la portée de la surveillance actuelle. Le premier exemple est tiré du monde des affaires et concerne l'entreprise Acxiom. Entreprise internationale d'agrégation de données, Acxiom fait la collecte de renseignements personnels sur des gens, dont des Canadiens, à partir de différentes sources puis elle les vend à des sociétés ou à des groupes politiques qui les utilisent pour faire du marketing ou pour faire campagne. Acxiom recueille un vaste éventail de renseignements, dont des données communes comme le nom,

l'adresse et le numéro de téléphone. Néanmoins, elle recueille et vend aussi des données de nature délicate, comme votre état matrimonial, votre âge, votre origine ethnique, la valeur de votre domicile, vos lectures, le type de voiture que vous conduisez, ce que vous commandez par téléphone ou Internet, l'endroit où vous allez en vacances, vos loisirs, vos antécédents de santé mentale, votre consommation d'alcool, et ainsi de suite. Même avant l'avènement des médias sociaux, Acxiom détenait une quantité phénoménale d'information, équivalente à une pile de livres de 80 000 km de haut[3]. Étant donné la popularité d'applications comme Facebook, qui ont révolutionné la quantité de données personnelles auxquelles ont accès les entreprises d'agrégation de données et d'autres organismes[4], cette quantité n'est plus du tout représentative du volume de données traité par Acxiom.

Le second exemple traite de la collecte et de l'analyse de renseignements provenant de sources électroniques, telles que des téléphones cellulaires et l'Internet, à des fins de sécurité nationale. Depuis les attentats terroristes du 11 septembre, le Canada et les États-Unis ont accru leurs échanges mutuels de renseignements. Bien que le processus demeure opaque, nous pouvons parfois entrevoir la quantité presque inimaginable d'information recueillie. Selon James Bamford, la National Security Agency étatsunienne s'attend à traiter d'ici 2015 une quantité stupéfiante d'information se comptant en yottaoctet, soit 10 octets à la puissance 24[5]. Si l'on imprimait ces données, cela correspondrait à un septillion ou un billion de billions de pages de texte. En 2011, combinés, tous les disques durs de la planète n'atteignaient pas un yottaoctet.

Dans ces deux exemples, il s'agit d'une surveillance de données effectuée au moyen d'ordinateurs, activité que les anglophones appellent « dataveillance ». Toutefois, afin de compléter le portrait de la surveillance, on doit également inclure les technologies comme les caméras, les drones, le dépistage des drogues, les lecteurs automatiques de plaques d'immatriculation, les téléphones intelligents et la biométrie (les technologies qui permettent d'identifier une personne en fonction de ses caractéristiques biologiques). La technique la plus connue est la prise d'empreintes digitales. Les systèmes biométriques d'aujourd'hui permettent toutefois d'identifier une personne à l'aide de son ADN, de la structure du visage, de la géométrie de la main, de la voix, de la démarche, de la rétine ou de l'iris. Conjugués, tous ces phénomènes produisent et continueront de produire une transformation radicale de toutes les sphères de la vie, dont le commerce, la conduite de la guerre, les sciences, la sécurité internationale, la santé, les soins à l'enfant, le

travail et les mécanismes officiels et non officiels qui servent à encourager les gens à se conformer aux attentes et aux règles sociétales (mécanismes souvent réunis sous l'appellation de « contrôle social »).

Il n'y a pas si longtemps, nous croyions que la surveillance se limitait au monde de l'espionnage ou visait principalement les criminels. Or, en réalité elle est utilisée depuis longtemps dans des domaines comme le travail et le commerce. Aujourd'hui, il est plus facile de constater que la surveillance est inévitable pour presque tout le monde. Consentir à être observé est devenu le compromis que nous devons faire pour jouir d'une réduction de prix ou d'une amélioration du service. Cela ne se réduit pas à un phénomène visuel et comprend maintenant l'utilisation de données électroniques. En réalité, nombre d'entre nous fournissons volontairement des données, car cela rend notre vie plus commode. Dans la section suivante, nous présentons une situation hypothétique pour montrer à quel point la surveillance fait maintenant partie intégrante de la vie de tous les jours des Canadiens et des habitants d'autres sociétés industrialisées.

Une journée dans la vie de Farah, une fillette de neuf ans

Farah remonte les couvertures par-dessus sa tête pour éviter encore un peu de déclencher la routine matinale où se succèdent petit-déjeuner et devoirs. En ouvrant les yeux, elle se souvient du programme de la journée. Aujourd'hui, elle recevra l'appareil que toute préadolescente rêve d'avoir et elle s'envolera vers un autre pays. Bien qu'elle soit accoutumée à ce genre de choses, elle reconnaîtra peut-être que sa journée montre à quel point sa vie et celle des personnes qui l'entourent sont devenues transparentes.

Elle se glisse hors du lit 40 minutes avant que l'alarme de son frère aîné ne retentisse dans la chambre d'à côté. En regardant par la fenêtre, elle croise le regard de sa voisine âgée, Mme Krupp, qui lui envoie la main. Elle et Farah ont fait connaissance au parc où Mme Krupp donne un coup de main avec d'autres adultes pour surveiller les enfants qui s'amusent dans les structures de jeux.

Farah et sa famille ont emménagé dans ce quartier de Mississauga il y a 18 mois. Ils ont acheté cette maison, car elle est située près d'une ligne d'autobus qui se rend directement au travail de sa maman, dans une petite entreprise de logiciels. Quant à son papa, il enseigne la physique à l'Université

de Toronto ; il a dû se résigner à rester coincé dans les embouteillages plusieurs fois par semaine pour se rendre au centre-ville.

Ce matin-là, son père est déjà au travail. Farah, qui ne veut pas réveiller sa mère, évite par habitude les planches qui craquent et qui signalent habituellement à ses parents qu'elle est sortie du lit. Toutefois, dernièrement, ils sont un peu moins vigilants, car sa maman a eu un bébé il y a deux mois, le petit Bruno. Né prématurément, il a été hospitalisé pendant plusieurs semaines pour que les médecins puissent faire des examens : gazométrie sanguine, radiographie des poumons et surveillance de ses fonctions cardiorespiratoires. Pendant la grossesse, ses parents se sont habitués à un suivi médical très étroit. Comme sa mère est âgée de plus de 40 ans, sa grossesse présentait davantage de risques. Par conséquent, Farah a souvent été confiée à Mme Krupp alors que sa mère devait se rendre à l'hôpital pour y passer une batterie de tests pour s'assurer que le bébé ne présentait aucune anomalie génétique et que son développement était normal.

Peu avant la naissance de Bruno, sa maman est arrivée à la maison avec une image de l'échographie en trois dimensions du bébé. Ses parents ont immédiatement ajouté la photo aux centaines d'autres photos de Farah et de son frère aîné sur la page Facebook de sa mère. Tout le monde parle de cette photo comme de la « première photo de Bruno », mais Farah ne pense pas que cette image lui ressemble ni d'ailleurs qu'elle ressemble à quiconque. Elle ne l'a pas regardée longtemps, car elle lui donne un peu la chair de poule.

C'est aussi à ce moment que son père a commencé à installer les choses pour le bébé ; il a notamment placé un berceau dans la chambre de Farah. Il a accroché sur le montant du berceau un nouvel interphone de surveillance. Cet appareil permet aux parents d'entendre Bruno, mais aussi de le voir sur un ordinateur ou un téléphone intelligent peu importe où ils sont sur la planète grâce à la caméra connectée à un système Wi-Fi. L'appareil est doté d'une fonction de vision nocturne et d'un zoom ainsi que d'un détecteur pour la température, l'humidité et les mouvements du bébé. Ses parents peuvent également utiliser l'interphone pour parler à distance au bébé. Farah se demande si ses parents utilisent parfois l'appareil pour *la* surveiller.

Elle descend l'escalier sur la pointe des pieds en se disant que c'est agréable de ne pas trébucher sur les vêtements ou les câbles d'ordinateur qui jonchent habituellement le sol. Bien qu'il soit épuisé, son père fait de gros efforts pour garder la maison plus ordonnée qu'à l'habitude. Selon Farah,



Une cible de choix des entreprises pour la collecte de données : les enfants. (Source : © iStockphoto.com/Brzi)

ces efforts sont dus aux quelques visites de l'infirmière de santé publique ; cette dernière vient à la maison pour s'assurer que Bruno et sa maman vont bien et elle surveille les signes de dépression postpartum ou de psychose. Ses parents comprennent la préoccupation, mais ne sont pas à l'aise avec la façon dont l'infirmière parcourt le salon et la cuisine pour voir s'il n'y aurait pas quelque chose qui cloche. Voilà pourquoi son père fait des efforts hors du commun pour garder la maison propre.

Lorsque Kay, le frère de Farah, se lèvera, il partira en vitesse à son entraînement de soccer. Farah pourra donc jouer sur l'ordinateur sans être dérangée. Elle aime bien les jeux gratuits en ligne ; elle ne s'attarde pas aux conséquences des conditions d'utilisation, par lesquelles elle autorise

Les jeux vidéo « voient » les joueurs dans leur salon

Les fabricants de jeux vidéo rivalisent pour offrir une expérience de jeu toujours plus réaliste, par exemple en permettant aux joueurs de contrôler la console au moyen de mouvements physiques naturels (danser ou sauter pour contrôler un personnage) plutôt que d'utiliser une manette. L'envers de la médaille est que, bien que ces jeux présentent un potentiel d'immersion beaucoup plus grand puisqu'ils intègrent des mouvements naturels au jeu, ils portent davantage atteinte à la vie privée puisqu'ils analysent le corps, les comportements et l'environnement des joueurs; les fabricants profitent ainsi d'une mine d'information personnelle.

La console Xbox 360 de Microsoft a été l'un des premiers systèmes à utiliser cette nouvelle technologie. Lancée par Microsoft en 2005, cette console est connectée à Internet et offre le service Xbox LIVE qui permet aux utilisateurs de jouer à des jeux en ligne avec d'autres, d'acheter des jeux dans un marché virtuel et de conserver leurs statistiques de jeu au moyen de trophées virtuels, appelés « accomplissements ».

Bien que la Xbox 360 soit dotée de multiples accessoires, dont un micro pour le clavardage vocal et d'une caméra Web pour le flux de données vidéo, le périphérique le plus intéressant est la Kinect. Lancé en 2010, ce capteur peut « voir » le corps du joueur, faire une distinction entre le joueur et les meubles et différencier les joueurs. L'appareil projette des rayons infrarouges devant lui. Le corps humain reflète ces rayons qui sont captés par la caméra infrarouge de la Kinect.

les fabricants à recueillir, entre autres, des renseignements sur son emplacement et son numéro de téléphone et voir le statut de leur réseau sans fil. Lorsqu'elle ouvre son jeu favori, le fabricant enregistre les détails de son comportement en ligne ; il utilisera ces renseignements pour développer de nouveaux produits et pour cibler leur mise en marché. L'entreprise vend également ces données à d'autres entreprises qui souhaitent en savoir le plus possible sur les habitudes de consommation des enfants. Farah joue à des jeux qui comprennent un questionnaire de personnalité et des enquêtes auprès des consommateurs ; en remplissant ces questionnaires ou ces enquêtes, les enfants obtiennent des points ou des privilèges supplémentaires.

Mais, pour le moment, Farah a faim. Pendant qu'elle prépare son déjeuner, elle remarque que sur la boîte de céréales on annonce un concours pour gagner des billets pour le concert de son *boy-band* favori.

Cette caméra permet de suivre le mouvement et de traduire les mouvements des joueurs dans le monde virtuel. La Kinect est devenue un atout si essentiel au plan marketing de Microsoft qu'elle sera incluse dans les nouvelles versions de la Xbox.

La capacité de « voir » de la Kinect sert également à repérer les réactions émotionnelles aux publicités. Si Farah, son frère ou un autre enfant dans le monde réel décide de regarder une vidéo ou une émission de télévision sur la Xbox 360, la Kinect fera jouer une publicité appelée « NUad » avant la projection. Pendant cette publicité, le système repère les réactions de l'utilisateur afin de vérifier s'il porte attention à la publicité. Microsoft vend ensuite les données (âge, race et sexe des joueurs) ainsi glanées auprès de millions d'utilisateurs par la Kinect et Xbox LIVE, ainsi que d'autres renseignements sur le comportement du joueur pendant la publicité à des publicitaires qui s'en servent pour faire des études de marché. Microsoft a aussi fait breveter la fonction de la Kinect qui empêche les gens de contrevenir aux conditions d'utilisation concernant le nombre de personnes qui peuvent regarder une vidéo ou jouer à un jeu. À titre d'exemple, si la Kinect « voit » plus de gens regarder une vidéo que ce que le permettent les conditions d'utilisation, elle arrêtera la lecture de la vidéo. Microsoft a-t-elle le droit d'adopter de telles conditions? Le potentiel croissant des technologies de détection pour l'application de la gestion des droits numériques dans le monde réel serait-il en train d'estomper la frontière entre les politiques d'entreprise et de marketing de Microsoft, d'une part, et le salon des consommateurs, d'autre part?

Il ne faut pas qu'elle oublie de demander à sa mère de l'inscrire. Sa mère devra aller sur le site Web de l'entreprise et entrer le code de produit unique inscrit sur la boîte de céréales. Elle devra aussi fournir des renseignements personnels. Avec le code de produit et cette information, le fabricant des céréales disposera de données précises sur le mode de vie et les habitudes de consommation de la famille. Il contribuera ainsi à une forme de marketing qui est de plus en plus ciblée étant donné la facilité avec laquelle on peut lier cette information aux données personnelles sur d'autres aspects de la vie des consommateurs.

Après s'être brossé les dents, Farah va sur sa page Facebook. Officiellement, elle est trop jeune pour avoir un compte, mais comme la plupart de ses amis, elle a menti sur son âge pour s'inscrire et est devenue une utilisatrice régulière. Chaque fragment d'information que Farah révèle sur Facebook – chaque événement, chaque chanson ou émission qu'elle « aime »,

chaque mise à jour de son statut et chaque photo – viennent s'ajouter à un gigantesque dépôt de données que l'entreprise vend à des tiers. En cas d'urgence, les services de police et les responsables de la sécurité auraient également accès à l'information qui figure sur sa page. Aujourd'hui, toutefois, il ne se passe pas beaucoup de choses, sauf son ami Josh qui se vante de sa nouvelle voiture-jouet. Comme il a indiqué le nom du fabricant dans son commentaire, celui-ci sera automatiquement sélectionné par des sociétés qui font de la récupération de données en ligne. Ces firmes recueillent et regroupent de façon invisible les commentaires de milliers d'utilisateurs à propos de sujets, de produits ou de services particuliers. Elles vendent ensuite ces données à des entreprises qui s'en servent pour connaître l'opinion des citoyens sur des produits, des organisations, des phénomènes ou des personnes. Ces mêmes firmes recueillent aussi les commentaires des gens sur des enjeux politiques ou sociaux qu'elles vendent ensuite à des stratèges politiques.

Comme Ariel, sa meilleure amie, n'a pas encore le droit d'aller sur Facebook, Farah utilise Gmail pour lui envoyer une photo amusante de leur chien. Encore une fois, bien que, selon les règles de Gmail, ils soient trop jeunes pour posséder un compte, Farah et ses amis ont simplement menti lorsqu'ils se sont inscrits. Ce qu'elle ne sait pas, c'est que le courriel qu'elle vient d'envoyer est scruté de façon automatisée à différents degrés par des agences mondiales de sécurité qui surveillent le flux des courriels. Si elle contactait des personnes suspectes ou utilisait certains mots ou certaines combinaisons de mots, ses messages seraient signalés, feraient l'objet d'un examen encore plus approfondi et seraient suivis par les responsables de la sécurité. D'ailleurs, son père a souvent fait observer que comme il est physicien nucléaire et qu'il a fait ses études en Iran, il est probable que ses messages ainsi que ceux de sa famille soient lus de façon régulière.

En sortant de la maison, Farah se dit que le paysage est bien différent en cette chaude journée de printemps que celui de la photo dans Google Street View, laquelle a été prise en janvier. Elle a appris l'existence de Street View la semaine dernière lorsqu'elle a vu une voiture au centre-ville avec une caméra sur le toit. Kay lui a alors montré quelques photos de leur quartier sur le système de cartes de Google. Il avait particulièrement hâte de lui montrer l'image de leur ami Lani (dont le visage a été caché) qui joue avec son chien devant la maison.

Lorsque Farah arrive à l'école, elle est filmée par l'une des caméras qui surveillent l'entrée. Les caméras ont été installées il y a quelques mois par le

directeur de l'école après qu'une série de graffitis eut été faite sur les murs de l'école*.

Farah se dépêche à se rendre à sa classe, car aujourd'hui ils passeront un examen standardisé. Elle est nerveuse, car elle souhaite avoir une bonne note ; son frère n'a pas obtenu un bon résultat et n'a pas pu s'inscrire à ses cours favoris à l'école secondaire. Farah ne veut pas se retrouver dans la même situation que Kay. La note qu'obtiendra Farah sera inscrite à son dossier pédagogique qui la suivra au moins jusqu'à l'âge adulte. L'examen sert également à évaluer la performance des enseignants. De plus, comme la concurrence augmente dans le milieu scolaire, les écoles s'en servent aussi comme un important instrument de promotion et les parents, pour évaluer les options en matière d'éducation.

Après l'examen, tous les élèves se précipitent à l'extérieur pour la récréation sous la surveillance des professeurs et d'un parent bénévole ; ce parent a dû faire l'objet d'une enquête de sécurité. Josh montre son nouveau jouet et souligne que ce qui rend la voiture vraiment *cool* est qu'elle est munie d'une petite caméra. Lorsqu'il est chez lui, il promène la voiture dans la maison et enregistre des images ; il a déjà téléchargé une vidéo sur leur ordinateur. Il a également utilisé la voiture pour espionner son frère et pour pourchasser son chat (qui est muni d'une micropuce lisible à la machine pour l'identifier), qui craint ce jouet. Josh est décu que les filles ne soient pas impressionnées lorsqu'il leur montre son bolide puisque plusieurs possèdent déjà une poupée « Barbie vidéo » qui est munie d'une caméra.

Le frère de Farah paie en argent comptant son déjeuner à la cafétéria aujourd'hui, mais il se pourrait que bientôt son argent n'y soit plus accepté. Selon une vaste tendance observée à l'échelle mondiale dans les écoles, les élèves paient pour leurs goûters et leurs repas au moyen d'un coupon électronique vérifié par un identifiant biométrique comme une empreinte digitale ou un balayage de l'iris. Ces systèmes éliminent les casse-têtes de

* Dans certains États américains, les enfants sont obligés de porter une carte d'identité munie d'une puce d'identification par radiofréquence, laquelle permet de limiter l'accès à certaines parties de l'école, de produire des rapports automatisés de présence et d'informer les responsables de l'école de l'endroit où se trouvent tous les enfants dans l'école en tout temps. Pour lutter contre l'obésité infantile, certaines écoles exigent même que la masse corporelle des élèves soit consignée dans le cadre du programme de santé. Il est commun d'installer des caméras dans les salles de classe ainsi que dans les corridors. De plus, certaines écoles exigent que les enfants passent par des détecteurs de métal. Plusieurs écoles canadiennes envisagent de prendre ce genre d'initiatives.

l'argent comptant et permettent aux parents de surveiller les achats faits sur le compte de leur enfant. Les parents peuvent même dresser une liste d'interdictions, comme les bonbons ou les aliments frits, que le système ne permettra pas aux enfants d'acheter.

Farah rentre à l'école et discute brièvement avec Mme Krupp qui est accompagnée de l'agent Garza, le policier qui travaille dans l'école secondaire adjacente. L'agent Garza sert de modèle de rôle et assure la sécurité en partie grâce au réseau informel d'informateurs qu'il entretient parmi les enfants.

De retour en classe, Farah travaille sur les ordinateurs de l'école. Alors qu'elle navigue sur différents sites Web, son comportement est surveillé automatiquement au moyen de fichiers témoins électroniques (*cookies*). Ces témoins enregistrent chaque visite sur un site Web et aident à cibler de mieux en mieux les publicités qui apparaissent à l'écran. Les professeurs surveillent de près les enfants pour s'assurer qu'ils ne consultent pas de sites inappropriés. Leur vigilance s'ajoute au logiciel de l'école qui fait le suivi des habitudes de navigation des élèves, bloque les sites jugés inappropriés et produit des rapports automatisés de leurs activités en ligne.

Au fur et à mesure que la journée avance, Farah n'arrive presque plus à contenir sa joie ; ce soir, toute la famille s'envolera vers Téhéran pour visiter la famille élargie. Bien que Farah ait pris l'avion à maintes reprises, c'est la première fois qu'elle remarque toute la paperasserie requise pour faire un voyage à l'étranger. Elle a vu son père demander un visa puis vérifier la date d'expiration sur le passeport de chacun. Elle a aussi entendu ses parents se plaindre d'avoir à se presser pour obtenir un passeport pour Bruno. Pour ce faire, ils ont dû cajoler le nouveau-né pour prendre une photo qui réponde aux exigences de Passeport Canada ; une drôle de situation !

Lorsqu'elle rentrera à la maison, ses parents l'attendront pour lui donner à l'avance son cadeau d'anniversaire. Elle sait déjà qu'ils ont accepté de lui acheter le téléphone intelligent pour lequel elle les a harcelés. Au début, ses parents n'étaient pas d'accord avec l'idée qu'une fillette de dix ans ait un téléphone portable. Ils ont toutefois changé d'idée quand ils ont appris les fonctions de géolocalisation des téléphones intelligents. Quand elle reçoit son cadeau, ses parents ont déjà installé un logiciel sur le téléphone pour localiser avec précision où se trouve Farah et pour suivre ses déplacements. Les inquiétudes de ses parents quant aux cyberrisques pour les enfants se sont également dissipées quand ils ont appris qu'ils pouvaient installer un logiciel qui fait déjà recette et qui leur permet d'avoir accès à tous les

courriels et messages textes de Farah, et de voir qui elle a appelé et quels sites elle a visités.

En arrivant à la maison, Kay dénonce l'injustice : *lui*, à l'âge de Farah, il n'avait pas le droit d'avoir un téléphone. Kay est un athlète de grand talent et il s'entraîne chaque jour dans l'espoir d'être sélectionné dans l'équipe junior de soccer du Canada. S'il est choisi, il devra se soumettre à des analyses de sang et d'urine au hasard*.

Tout le monde s'affaire aux derniers préparatifs pour le voyage. Avec les nouvelles mesures de sécurité prises depuis les attentats terroristes du 11 septembre, le père de Farah est obsédé par le fait d'arriver vraiment très tôt à l'aéroport. Compte tenu de sa profession, de ses origines iraniennes et de ses voyages fréquents au Moyen-Orient, il craint d'être inscrit par inadvertance sur la liste des personnes interdites de vol lors du précontrôle des passagers. Comme le nom de famille « Farad » est très répandu en Iran, il y aurait plus de risques qu'il y ait erreur sur la personne. Il préfère donc avoir suffisamment de temps pour régler les problèmes si jamais il devait y avoir une confusion.

Le taxi arrive et la mère de Farah arme le système d'alarme de la maison ; ses parents ont toujours eu un système d'alarme depuis la naissance de Farah. Récemment, ils sont toutefois passés à un service supérieur qui permet de détecter les intrusions, les incendies, le monoxyde de carbone et les inondations. Des caméras ont également été installées grâce auxquelles on peut surveiller les entrées à partir d'un ordinateur ou d'un téléphone intelligent de n'importe où sur la planète. Tout ce dont on a besoin est d'une connexion Internet. Lors de son dernier voyage en Turquie, son père a utilisé son téléphone intelligent pour regarder les enfants partir pour l'école directement de sa chambre d'hôtel surplombant le Bosphore.

Alors que la famille de Farah s'entasse dans le taxi, ses membres sont photographiés par une petite caméra installée près du pare-brise. Sur le chemin de l'aéroport, des images du taxi sont également prises par les caméras de surveillance de la circulation. Pour éviter les embouteillages de l'heure de pointe, le conducteur du taxi prend la sortie vers l'autoroute à péage électronique. Des capteurs surélevés se connectent au transpondeur du taxi, un appareil électronique qui permet à l'entreprise de péage d'identifier

* Certaines écoles aux États-Unis exigent que tous les enfants qui souhaitent participer à des sports extrascolaires se soumettent à des tests de dépistage des drogues.

automatiquement chaque véhicule dès qu'il s'engage sur une autoroute à péage. L'entreprise peut ainsi calculer le montant du péage. Le père de Farah ne s'est jamais soucié d'installer un transpondeur dans la voiture familiale. Alors, lorsqu'il emprunte cette autoroute, c'est un système de lecture automatique des plaques d'immatriculation qui lit la plaque et produit une facture.

Une fois au terminal, le père de Farah paie le taxi au moyen de sa carte de crédit. Cette transaction devient alors une infime partie du grand profil financier de son père et vient influencer sa cote de solvabilité. Toute la famille décharge les bagages sous le regard des policiers et des caméras de sécurité qui foisonnent dans l'aéroport. Certaines de ces caméras sont si perfectionnées qu'elles peuvent lire à distance les messages textes sur son nouveau téléphone. Néanmoins, elles seront bientôt remplacées par des caméras munies de microphones qui permettront aux agents de sécurité d'écouter et d'enregistrer furtivement les conversations.

Le père de Farah fait imprimer les cartes d'embarquement de toute la famille à un poste automatisé libre-service et remet les documents de voyage de la famille à un agent. Un chien renifleur se promène tranquillement alors qu'ils placent leurs bagages sur le convoyeur. Bruno est agité alors qu'ils attendent dans la file qui serpente jusqu'à la sécurité. Les parents de Farah se demandent alors s'ils ne devraient pas s'inscrire au programme Nexus cette année. Ils pourraient ainsi passer plus rapidement les contrôles de sécurité. Ils devraient toutefois payer des droits de traitement et donner encore plus de renseignements personnels aux agents des services frontaliers, notamment leurs antécédents professionnels, leurs habitudes de déplacements et, le cas échéant, leur casier judiciaire.

Arrivée au contrôle de sécurité, les agents vérifient une fois de plus leur passeport alors que les Farad mettent leur bagage à main dans l'appareil de radioscopie. Tout le monde doit ensuite passer au détecteur de métal. Le père de Farah porte le bébé dans ses bras ; Bruno ne semble pas très content de quitter sa poussette. On effectue un prélèvement sur le sac à dos de Kay pour vérifier qu'il ne contient pas d'explosifs. Chacun des membres de la famille passe ensuite au scanneur corporel, lequel produit une image très précise comme s'ils n'avaient pas de vêtements. Pour ce voyage, ils n'ont pas eu à passer au lecteur d'empreintes digitales puisque, lors d'un long séjour en Californie l'an dernier pendant que le père de Farah profitait d'une année sabbatique à l'Université Stanford, les données sur leurs empreintes digitales ont été stockées dans le système américain de sécurité frontalière. Lorsqu'ils prendront leur vol de correspondance à l'aéroport Heathrow de



Formes de surveillance qui sont maintenant d'usage dans les aéroports (Source : © iStockphoto.com/EdStock)

Londres, leur visage sera également balayé au moyen d'un logiciel de reconnaissance faciale. La mère de Farah chuchote à son conjoint qu'elle est ravie que, cette fois-ci, personne n'ait été sélectionné pour des vérifications encore plus accaparantes.

La mère de Farah range son ordinateur portable dans sa mallette. Son père remet Bruno dans sa poussette et tous remettent souliers et ceinture. Ils se rendent ensuite au salon privé ; sa mère fouille parmi son jeu de cartes de fidélité pour trouver celle qui leur permettra d'entrer. Sa mère possède une carte, entre autres, pour l'essence, l'épicerie, les hôtels, le café et les produits de beauté. Chaque carte lui donne droit à des avantages et à des rabais et s'inscrit dans la nouvelle économie de l'information qui repose sur l'enregistrement minutieux des habitudes de consommation de chacun des détenteurs. Ces renseignements sont maintenant essentiels à la prise de décisions commerciales au sujet du développement de produit, de l'établissement des prix ou de l'emplacement des succursales.

Les rayons du soleil couchant illuminent la cabine alors qu'ils se rendent à leur siège. Sans qu'ils le sachent, un policier des airs de la GRC qui est infiltré inspecte furtivement tous les passagers bien assis dans son siège près de la sortie de secours.

Bientôt, Farah et sa famille survoleront le Canada, mais ils laissent en quelque sorte des traces de chacun d'eux derrière ; ces traces prennent la forme de profils d'information de plus en plus vastes et élaborés. Ils se composent de textes et d'images et sont maintenant essentiels au fonctionnement des sociétés contemporaines. Cette journée dans la vie de Farah était bien occupée, mais peu remarquable. Pendant cette journée, sa famille et elle ont été surveillées par différentes personnes et différents organismes. La famille de Farah est relativement privilégiée et possède donc un profil de surveillance distinct qui est centré surtout sur la consommation et la sécurité personnelle. Peu importe la position que nous occupons dans la société, nous pouvons tous nous attendre à faire l'objet d'examens approfondis plus nombreux et variés qu'autrefois. Et cette tendance se poursuivra et s'accentuera.

On pourrait expliquer la surveillance dont fait l'objet Farah par le fait qu'elle est une enfant et que l'on s'attend à ce que les enfants soient surveillés. Or, plus elle vieillira, plus Farah sera surveillée. En effet, en vieillissant, elle nouera des liens avec tout un éventail de nouveaux organismes. Lorsqu'elle commencera à conduire, à travailler, à utiliser des services financiers, à voyager, à faire du sport et à bénéficier des services sociaux, de nouveaux organismes la surveilleront. Par ailleurs, si elle a des problèmes médicaux ou si elle se prend dans les mailles du système de justice pénale, elle sera soumise à d'autres formes de surveillance. Au fur et à mesure qu'elle étudiera, son dossier pédagogique grossira et prendra de l'importance. Nous pourrions même penser que certains des projets futuristes de publicités interactives et de drones munis de caméra de sécurité se concrétiseront au courant de sa vie. Son monde sera envahi par la surveillance ; cette surveillance créera de nouvelles possibilités, mais menacera également de submerger les régimes actuels de protection de la vie privée et nous poussera tous à réfléchir à la façon dont nous devrions vivre avec cette fenêtre ouverte sur notre vie privée.

L'augmentation de la surveillance mise en contexte

La section sur « une journée dans la vie de Farah » nous donne une idée des différentes formes de surveillance qui deviennent de plus en plus communes et qui touchent de plus en plus de sphères de notre vie quotidienne. Or, l'histoire évite également nombre de questions que l'on doit se poser pour obtenir un portrait complet et critique des enjeux soulevés par cette augmentation et cette intensification de la surveillance. Le reste de l'ouvrage portera sur ces questions ; nous verrons que certaines sont plus alarmantes que d'autres.

Tout d'abord, dans cette histoire, on ne dit pas si toute cette surveillance donne les résultats escomptés. Voilà une question essentielle ; on demande trop souvent au public d'avoir la certitude que la surveillance donnera les résultats annoncés. Or, d'importantes questions quant à l'efficacité d'une si grande surveillance demeurent sans réponse. Prenons l'un des exemples les plus flagrants, soit l'expansion mondiale de la surveillance pour la lutte contre le terrorisme. Cette surveillance peut contrecarrer certaines attaques terroristes, mais elle ne peut réellement réduire dans l'ensemble cette grande menace si l'on ne remédie pas aux conditions sociales, politiques et économiques qui sont à l'origine du terrorisme.

Concrètement, on ne sait pas si le réseau grandissant de caméras de surveillance contribue réellement à réduire la criminalité. Les preuves de la contribution des caméras à la lutte contre la criminalité sont extrêmement ambiguës et, dans bien des cas, il est évident que ces mesures sont loin de produire le type de réduction de la criminalité prévu[6]. Par ailleurs, même quand les caméras permettent d'attraper certains contrevenants, elles ne représentent pas nécessairement une utilisation judicieuse des ressources. Les données les plus détaillées sur le sujet nous proviennent du Royaume-Uni, où ont été installées plus de caméras que dans tout autre pays occidental. Selon un rapport de la police métropolitaine de Londres, qui était l'un des principaux défenseurs des caméras de surveillance, il faudrait mille caméras pour attraper un seul criminel[7]. De plus en plus de preuves font état de la piètre performance des caméras de surveillance pour réduire la criminalité ; il est donc intrigant que les responsables de la sécurité commencent maintenant à justifier l'utilisation de caméras de sécurité en affirmant qu'elles donnent aux gens un sentiment de sécurité. Sans compter que cette nouvelle affirmation n'est pas davantage démontrée que l'autre.

D'ailleurs, même en se demandant si les systèmes de surveillance sont réellement efficaces, on passe à côté de l'essentiel puisqu'on ne tient



Voiture de police munie d'une caméra (Source : © iStockphoto.com/Antonprado)

pas compte des facteurs qui motivent leur installation. Bien que les responsables puissent clamer que les mesures de surveillance sont adoptées pour renforcer la sécurité ou l'efficacité, l'attrait principal pour les décideurs est souvent le désir d'avoir l'air moderne et de sembler s'attaquer à des problèmes intraitables comme la criminalité et le désordre, peu importe si les mesures choisies sont réellement efficaces[8].

Toutefois, l'expansion de la surveillance entraîne un risque d'erreurs systématiques et cumulatives. Les défenseurs de la surveillance parlent généralement de ces systèmes comme s'ils étaient sans faille, mais force est de constater que tous les systèmes de surveillance présentent des défaillances et des erreurs courantes et que les organismes déploient beaucoup d'efforts pour les repérer et en diminuer le nombre. Parfois, les systèmes contiennent de telles erreurs chroniques sur le plan des données personnelles que les organismes ne prétendent même plus qu'ils sont exacts. C'est le cas pour les bases de données de la police sur les criminels et les rapports

de solvabilité des consommateurs ; ceux-ci tendent à être bourrés d'erreurs qui ne sont pas corrigées et qui sont difficiles à rectifier. Cette information est particulièrement déconcertante puisque ces systèmes jouent un rôle important en façonnant les possibilités qui s'offrent aux gens au cours de leur vie.

La prédominance accrue de la surveillance est importante non seulement pour sa capacité à suivre et à identifier les suspects, mais également pour sa capacité à modifier les comportements de toute la population. Même si la caméra n'enregistre pas ou que la fonction de géolocalisation n'est pas activée sur votre téléphone cellulaire, le fait de vivre dans un monde imprégné de surveillance modifie subtilement notre façon d'agir, nos propos et nos publications sur les médias sociaux. D'une certaine façon, nous nous autocensurons, ce qui a un effet paralysant et nuit au discours et à l'action politiques.

Par ailleurs, l'histoire de Farah et de sa famille ne montre pas non plus comment résister à la surveillance. Les gens critiquent souvent certaines des mesures de surveillance et tentent parfois d'éliminer ou d'atténuer celles qu'ils perçoivent comme volontairement nuisibles ou injustifiées. Pour ce faire, ils peuvent notamment avoir recours à des mesures juridiques pour contester la constitutionnalité d'une initiative ou pour la porter à l'attention des différents commissaires à la vie privée. Ces stratégies officielles peuvent à l'occasion contrer certaines mesures de surveillance. À titre d'exemple, des groupes canadiens de revendication, comme la British Columbia Civil Liberties Association et la Clinique d'intérêt public et de politique d'Internet du Canada, sont parvenus à traduire l'État ou des sociétés transnationales devant les tribunaux ou devant différents commissaires à l'information et à la vie privée[9]. Néanmoins, de graves questions demeurent sans réponse. Les dispositions législatives sur la protection de la vie privée en vigueur au Canada peuvent-elles réellement contrôler l'expansion générale de la surveillance dans presque tous les segments de la société ?[10]

En somme, l'histoire de Farah ne nous dit pas comment ont été créés les divers systèmes de surveillance ni comment ils ont pris de l'expansion. À l'exception de quelques initiatives de surveillance dont on a beaucoup parlé, l'accentuation de la majorité des mesures de surveillance fait rarement l'objet d'un débat public. C'est surtout parce que l'intensification se produit généralement par un processus de « glissement », c'est-à-dire par l'augmentation de la portée des pratiques existantes pour inclure des groupes et des régions qui n'étaient pas initialement visés. Les décisions au

Violations de données en série…

Plus notre information est capturée et communiquée, plus elle risque d'être perdue. Les violations de données, qui font maintenant la manchette dans tous les pays avancés, se produisent lorsque des données personnelles sur les consommateurs, les patients, les clients ou les employés sont volées ou, plus probablement, égarées par négligence ou communiquées par erreur. Les cas d'ordinateurs portables ou de périphériques de stockage perdus attirent l'attention des gens ordinaires sur les conséquences concrètes de la société de la surveillance dans laquelle ils vivent.

Bon nombre des cas de violation de données ont été très médiatisés au cours des dernières années au Canada. En 2013, notamment, un employé du ministère des Ressources humaines et du Développement des compétences du Canada a perdu une clé USB non cryptée, laquelle contenait les renseignements personnels de plus d'un demi-million de Canadiens, dont les numéros d'assurance sociale et des renseignements médicaux. De plus, selon des documents des Comptes publics du Canada, outre les clés USB, plus de 400 ordinateurs portables et BlackBerry appartenant à un vaste éventail de ministères ont été perdus ou volés au cours de l'exercice 2012-2013. Depuis 2002, 3 143 violations de données se sont produites dans les organismes fédéraux et elles toucheraient plus de 700 000 particuliers. Seuls 13 % de ces violations ont été signalées au Commissariat à la protection de la vie privée du Canada[1]. En raison du manque de transparence de la part des organismes responsables de la protection de notre information, la capacité du chien de garde fédéral de protéger notre information est limitée. Nous avons également été témoins de violations de données de la part d'organismes gouvernementaux provinciaux, d'hôpitaux, d'universités et d'autres types d'entreprises. Aucune institution n'est à l'abri.

En cas de violation de données, il est impossible de savoir à quoi serviront les renseignements ou à qui ils pourraient être transmis ou vendus. Les fraudeurs à l'identité peuvent notamment utiliser des données personnelles isolées et les combiner avec d'autres pour avoir accès à nos comptes bancaires ou à nos cartes de crédit. Ces violations minent également les intérêts et la réputation des organismes; bon nombre d'entre eux consacrent des ressources

sujet de ce changement d'orientation sont généralement hermétiques pour le public ; elles sont prises derrière des portes closes au sein des organismes. Le Royaume-Uni, l'un des pays les plus surveillés dans le monde, a connu deux exemples emblématiques de glissement de la surveillance qui peuvent

importantes pour former le personnel, pour s'assurer que les appareils mobiles sont adéquatement protégés par mot de passe et pour crypter rigoureusement les données personnelles. Or, les violations de données continuent de se produire de manière régulière, ce qui est très préoccupant.

Certains pays se sont dotés de lois robustes sur la violation des données, qui prévoient des sanctions sévères pour les violations graves. Parmi ces lois, certaines exigent l'envoi de lettres de notification et d'excuses à toutes les personnes qui pourraient être concernées par la violation. D'autres imposent des exigences strictes de signalement des violations à l'organe de réglementation de la vie privée compétent; si les risques sont suffisamment élevés, ce dernier peut alors obliger l'organisme fautif à communiquer avec toutes les personnes concernées.

Au Canada, toutefois, les exigences de signalement des violations des données sont encore essentiellement volontaires. L'Alberta est la seule province qui a imposé une obligation en vertu de la loi, selon laquelle les organismes du secteur privé doivent communiquer les violations des données portant atteinte à la vie privée. De plus, conformément à la *Loi sur la protection des renseignements personnels sur la santé* en Ontario, les organismes doivent avertir le commissaire à la première occasion. Au fédéral, le projet de loi C-12, qui devait modifier la *Loi sur la protection des renseignements personnels et les documents électroniques* et renforcer les exigences de signalement des violations des données, a été déposé en 2010. Or, il n'a toujours pas été mis à exécution. Le Canada a terriblement besoin de se doter de lois et de sanctions plus rigoureuses à cet égard. En l'absence de mesures de protection énergiques, des citoyens ont pris les choses en main; en 2012, certains ont notamment poursuivi en justice l'hôpital d'Ottawa et réclament 40 millions de dollars pour la perte d'une clé USB, laquelle contenait les données de 25 000 patients[2].

1. Laura Kane, « Privacy Watchdog Wants Ottawa to Force Companies to Report Release of Personal Data », *Toronto Star*, 23 mai 2013, http://www.thestar.com/news/canada/2013/05/23/privacy_watchdog_wants_ottawa_to_force_companies_to_report_release_of_personal_data.html.
2. Jordan Press, « Government Data Breached Thousands of Times in Last Decade, Documents Say », *Canada.com*, 23 avril 2013, http://o.canada.com/2013/04/23/government-data-breached-thousands-of-times-in-last-decade-documents-say/.

nous en apprendre beaucoup au moment où la surveillance est de plus en plus intégrée aux pratiques et aux politiques au Canada.

Le premier exemple est l'élargissement de la base de données génétiques de la police. Au début de la collecte d'ADN, les services de police et les

politiciens britanniques se sont confondus en promesses et se sont engagés à ne recueillir que l'ADN des « pires des pires » criminels, soit les terroristes et les pédophiles. Au fil du temps, ces promesses ont fini par être oubliées. Les policiers et les procureurs ont commencé à reconnaître qu'il serait commode d'élargir la base de données et d'inclure l'ADN d'autres catégories de délinquants puis de tous ceux qui sont accusés d'un crime, peu importe la gravité. Aujourd'hui, les policiers britanniques sont autorisés à recueillir, analyser et consigner l'ADN de quiconque est *suspect* d'être impliqué dans un crime. En pratique, ce pouvoir donne aux policiers une très grande latitude quant aux individus à inscrire dans la base de données.

Le second exemple de glissement de la surveillance concerne l'installation de caméras de surveillance dans les municipalités britanniques. Cet exemple nous montre qu'un système qui est conçu et autorisé pour un objectif particulier peut rapidement être associé à d'autres usages courants. À l'origine, le système de vidéosurveillance a été mis en place en vertu des dispositions législatives de lutte contre le terrorisme. Cependant, les autorités se sont vite aperçues qu'il y avait peu d'activités terroristes visibles dans les quartiers tranquilles du Royaume-Uni. Par conséquent, les administrations municipales ont commencé à utiliser le réseau de caméras à d'autres fins. Les opérateurs se sont donc mis à surveiller des écarts de conduite banals comme les gens qui urinent en public, les mineurs qui fument, les individus qui jettent des déchets par terre, ceux qui ne ramassent pas les excréments de leur chien et les livreurs de journaux sans permis. Bien qu'on ne puisse nier qu'il s'agisse là de désagréments quotidiens, il y a fort à parier que le public n'aurait pas appuyé l'installation d'un vaste réseau de caméras de surveillance aussi coûteux, si on lui avait dit qu'il servirait à s'assurer que les gens placent leur bac de recyclage sur le bord du chemin la bonne journée.

Conclusion

Bien que les Canadiens ne soient pas entièrement d'accord sur le bien-fondé de certaines mesures de surveillance, il faut souligner que la surveillance est une forme de pouvoir et que ce pouvoir peut s'exercer sur des individus spécifiquement identifiés ou permettre de manipuler des populations entières. Par ailleurs, l'expansion actuelle de la surveillance, qui fait de plus en plus partie intégrante de notre vie quotidienne, représente un renversement

formidable du rapport de force entre les citoyens et les organismes. Le plus grand danger de tout ce phénomène ne réside pas par conséquent dans le caractère intrusif d'une mesure de surveillance ou dans la possibilité que des erreurs soient commises dans l'identification ou le traitement des personnes, ni même dans la perte possible de données. Le plus important danger découle du simple fait que, petit à petit, nous créons une société dans laquelle la surveillance est profondément ancrée et que les mesures de surveillance peuvent facilement devenir des mesures d'oppression. Et, malheureusement, il est impossible de mesurer l'ampleur de ce danger. Notre infrastructure de surveillance sera une ressource que nous léguerons aux générations futures de politiciens, de chefs d'entreprise ou même de leaders messianiques. Il ne faudra qu'une volonté politique suffisante pour que cette infrastructure de surveillance change d'objectif et qu'elle serve à surveiller dans les moindres détails des gens dérangeants aux yeux de certains en raison de leurs opinions politiques, de leurs croyances religieuses, de la couleur de leur peau, de leur sexe, de leur statut migratoire, de leurs antécédents médicaux ou d'un nombre quasi infini d'autres facteurs qui ont été utilisés au cours de l'histoire pour braquer les gens les uns contre les autres. Certes, on pourrait rejeter ce scénario puisqu'il semble verser dans la « théorie du complot ». Or, il n'est pas nécessaire de croire que des forces secrètes tirent les ficelles pour reconnaître que nos systèmes de transparence en croissance constante posent des dangers bien réels et inquiétants.

Notes

1 Pour le premier, voir John L. Locke, *Eavesdropping: An Intimate History* (Oxford, Oxford University Press, 2010) ; pour le second, voir Kirstie Ball, « Workplace Surveillance: An Overview », *Labor History* 51, nº 1 (2010), p. 87-106 ; et Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (New York, St. Martin's, 1990).

2 Voir, par exemple, Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence, University Press of Kansas, 2007) ; Kevin D. Haggerty et Richard V. Ericson. *The New Politics of Surveillance and Visibility* (Toronto, University of Toronto Press, 2006) ; Torin Monahan, *Surveillance in the Time of Insecurity* (New Brunswick, NJ, Rutgers University Press, 2010) ; et Daniel Solove, *The Digital Person* (New York, New York University Press, 2006).

3 Robert O'Harrow, Jr., *No Place to Hide* (New York, Free Press, 2005). L'entrepôt de données d'Acxiom peut contenir jusqu'à un pétaoctet d'information, ou un milliard de millions d'octets. L'image d'une pile de bibles, utilisée par un officiel d'Acxiom, est donc basée sur une approximation voulant qu'une bible soit équivalente à un million d'octets d'information (Mo). Voir la note dans O'Harrow page 37.

4 Pour les médias sociaux et les données personnelles, voir Daniel Trottier, *Social Media as Surveillance* (Londres, Ashgate, 2012).

5 James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York, Anchor, 2009).

6 Martin Gill et Angela Spriggs, « Assessing the Impact of CCTV », *Home Office Research Study 292,* (Londres, Home Office Research, Development and Statistics Directorate, 2005), https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf.

7 Christopher Hope, « 1000 CCTV Cameras to Solve Just One Crime, Met Police Admits », *The Telegraph*, Royaume-Uni, 25 août 2009, http://www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html.

8 Kevin D. Haggerty et Camille Tokar, « Signifying Security: On the Institutional Appeals of Nightclub ID Scanning Systems », *Space and Culture* 15, nº 1 (2012), p. 124-134.

9 Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA, MIT Press, 2008).

10 James B. Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford, Oxford University Press, 2007).



Sécurisation et surveillance

Du droit à la vie privée aux risques pour la sécurité

Dans les dernières années, l'un des principaux moteurs de la croissance de la surveillance au Canada a été la priorité que nous accordons collectivement à la gestion du risque et à la sécurité. Ironiquement, bien que les Canadiens ordinaires doivent faire face à des risques de sécurité et de santé ainsi qu'à des risques financiers, ils sont en moyenne probablement plus en sécurité et dans une meilleure situation qu'auparavant. À titre d'exemple, l'espérance de vie moyenne au nouveau millénaire a dépassé l'âge de 80 ans[1]. Alors, pourquoi les Canadiens se préoccupent-ils autant des risques et de leur sécurité depuis le début de la seconde décennie du XXI[e] siècle ? Les attentats du 11 septembre ne peuvent expliquer à eux seuls cette inquiétude. Bien qu'ils aient imprimé un élan fondamental au renforcement de la sécurité, la campagne pour la gestion du risque et le renforcement de la sécurité avait commencé avant cette date et va bien au-delà de la lutte contre le terrorisme. Nous examinerons maintenant certaines des raisons qui expliquent cette importance accrue accordée au risque et présenterons des exemples qui ont mené à la prise de nouvelles mesures de surveillance ou au renforcement de celles-ci. Or, cette surveillance crée elle-même de nouveaux risques pour la protection des renseignements personnels, l'équité et la liberté.

Apprendre à connaître les élèves du Conseil scolaire du district d'Ottawa-Carleton

En 2010, le Conseil scolaire du district d'Ottawa-Carleton a informé les parents qu'il procéderait à un sondage auprès de tous les élèves, de la prématernelle à la douzième année, afin de recueillir des renseignements détaillés sur, entre autres, la vie de famille, la religion, l'orientation sexuelle, l'origine ethnique, les cas d'intimidation et de harcèlement pour chaque enfant.

Le Conseil scolaire avait alors indiqué qu'il avait besoin de cette information pour mieux déterminer et atténuer les risques auxquels chacun des enfants pourrait être exposé à l'école. Ce sondage a déclenché un tollé public puisqu'à proprement parler, il portait atteinte à la vie privée. Le Conseil a donc fait marche arrière et a mené le sondage sur une base volontaire. Il a également accepté d'interroger les parents des enfants d'âge primaire plutôt que les enfants eux-mêmes puisque les questions étaient de nature délicate. Toutefois, bien que le Conseil scolaire se soit engagé à assurer la confidentialité de cette information, les réponses n'étaient pas anonymes. En effet, chaque réponse était liée à un identifiant unique pour que le Conseil puisse identifier les enfants et mener des interventions après l'analyse des données.

Barrie Hammond, directeur de l'enseignement du Conseil, a défendu le sondage en soulignant qu'il s'agissait d'un important outil pour renforcer la sécurité. Il avait alors indiqué que plus ils en sauraient sur les élèves, plus ils connaîtraient leurs besoins, plus ils seraient en mesure de faire de l'école un endroit plus sûr[1].

1. « School Board Survey Gets Mixed Reaction », *CTV News*, 4 novembre 2010, http://ottawa.ctvnews.ca/school-board-survey-gets-mixed-reaction-1.570748.

Quelles sont nos craintes ? Quel est notre objectif ? L'évolution de la notion de risque et de sécurité

Depuis le début des années 1980, le risque est un mot clé. La notion de risque est importante non seulement pour le gouvernement et les entreprises, mais également dans le débat public et la recherche universitaire. C'est aussi à cette époque que l'on a vu l'apparition des professionnels de la gestion du risque et l'élaboration de plans et de techniques de gestion du risque de plus en plus complexes au sein du gouvernement, des entreprises et d'autres organismes. En fait, une grande partie de la vie moderne est organisée en fonction du risque[2]. La modernisation repose en partie sur le déploiement de méthodes systématiques de calcul et de gestion des risques. Ces méthodes



Sécurité et vie privée : un équilibre? (Source : © iStockphoto.com/rappensuncle)

nous permettent de nous gouverner en appliquant un raisonnement scientifique. D'ailleurs, les statistiques sont un outil fondamental de l'arsenal utilisé pour la gestion du risque ; elles servent souvent à prédire le comportement humain. Enfin, dans une société axée sur le risque, il est de plus en plus important de recueillir des données – toujours plus de données – sur notre comportement et les risques auxquels nous faisons face.

Avec cette priorité accordée au risque, la sécurité est devenue primordiale. Habituellement, lorsque nous pensons à la sécurité, nous pensons à la protection de la sécurité nationale contre des menaces comme le terrorisme, en particulier depuis le 11 septembre, et à la sécurité sociale qui est potentiellement assurée par les gouvernements. Or, la notion de sécurité s'est élargie depuis les années 1980 et englobe maintenant des secteurs,

tels que la sécurité environnementale, la sécurité alimentaire. Des comportements que l'on considérait autrefois comme banals sont maintenant jugés trop risqués et ne sont plus tolérés. À titre d'exemple, les nouveaux parents ne peuvent partir d'un hôpital canadien sans placer le nouveau-né dans un siège de sécurité pour bébé en raison du risque statistique de blessure en cas d'accident. Des lois ont notamment été adoptées dans sept provinces canadiennes pour obliger les cyclistes à porter un casque en vue de réduire le risque de lésion cérébrale en cas de chute. Et les parents sont incités par les autorités sanitaires et les écoles à enduire leurs enfants d'écran solaire en raison des risques de cancer de la peau. Ces exemples nous montrent que non seulement les lois ont changé, mais que notre notion de bon sens quant à ce qui est risqué et ce qui ne l'est pas a également évolué.

L'augmentation de la surveillance est allée de pair avec l'intensification des inquiétudes par rapport au risque pour deux raisons. Tout d'abord, la soif de données pour alimenter le calcul du risque a affaibli les normes de protection de la vie privée qui obligeaient traditionnellement les tiers, plus particulièrement les chercheurs scientifiques, à demander l'autorisation avant de recueillir des renseignements personnels. Nombre de provinces ont d'ailleurs adopté des dispositions pour la protection des renseignements médicaux qui permettent aux chercheurs en santé d'utiliser dans le cadre de leurs recherches des renseignements personnels sans obtenir le consentement lorsqu'il est impossible de le demander aux patients. Comme la collecte d'information sert à déterminer et à réduire les risques pour la santé, on lui donne préséance sur la protection de la vie privée. L'enquête sur la vie privée des élèves proposée par le Conseil scolaire de district d'Ottawa-Carleton (se reporter à l'encadré) est un autre exemple de l'application de cette logique.

Ensuite, une fois les risques déterminés, il est logique de surveiller les gens pour s'assurer qu'ils n'aient pas de comportements à risque et pour gérer les conséquences de ces comportements. Par exemple, le gouvernement fédéral fait le suivi des Canadiens qui quittent le pays afin de réduire la fraude ; si un bénéficiaire de prestations d'assurance-emploi part en vacances, il n'est donc pas disponible pour travailler. De la même façon, les compagnies d'assurance-vie demandent maintenant aux clients d'indiquer s'ils fument ou consomment de l'alcool. Elles utilisent cette information pour déterminer le type de couverture à laquelle peuvent souscrire les clients et le prix. Et elles refusent simplement d'assurer certaines personnes qui ont des problèmes de santé, comme le diabète ou un cancer, car le risque d'aggravation de leur état de santé est trop élevé.

Encore une fois, la surveillance est utilisée à des fins de précaution ou de contrôle. Il est toutefois important de noter que dans ce contexte, une société axée sur le risque et la sécurité peut facilement avoir recours à la surveillance pour mieux comprendre et mieux gérer les comportements qui sont considérés comme risqués.

L'augmentation des risques se traduit par une diminution de la confiance

Paradoxalement, en accordant une si grande place à la sécurité, on peut créer de l'insécurité. Bien que nous déployions de plus en plus d'efforts pour les gérer, les risques semblent être de plus en plus hors de notre contrôle. Comme notre société perçoit les risques comme un élément omniprésent, elle déploie des efforts inouïs pour les contrôler. Et plus nous réfléchissons aux risques et plus nous en discutons, plus nous créons un climat de doute et de peur ; nous avons donc besoin d'approfondir notre connaissance du risque. Nous sommes pris dans un cercle vicieux, qui justifie en partie le recours à la surveillance dans notre quête de sécurité.

Comme nous l'avons mentionné, cette notion accrue du risque et de la peur est paradoxale : bien qu'en moyenne, nous soyons probablement mieux protégés qu'auparavant, nous avons tendance à nous attarder sur les risques qui persistent. La stabilité de l'emploi a diminué et la précarité a augmenté, le filet de sécurité sociale du gouvernement s'effiloche et les Canadiens doivent affronter une série de nouveaux risques sociaux et technologiques. Les choses semblent évoluer rapidement. Il y a là une rupture avec les certitudes et les institutions traditionnelles, comme la famille. On vit maintenant notre vie de façon individuelle et on a l'impression que l'on est seul pour se défendre dans ce monde dangereux. Plutôt que de s'en tenir aux méthodes conventionnelles, nous tentons d'aider les individus à mieux comprendre et à protéger leur avenir contre tous les types de risques.

Par ailleurs, notre vision du risque est influencée par la mondialisation et par les liens de plus en plus nombreux qui se tissent entre le Canada et le reste du monde (se reporter à la Tendance 6). Ce facteur contribue également à accélérer le rythme des changements et à accentuer le climat d'incertitude. Plus les gens voyagent à l'étranger, plus l'on surveille les voyageurs pour repérer les terroristes ou les porteurs de maladie comme le H1N1. Une fois de plus, on assiste à une prolifération des risques et on doit accroître la surveillance pour renforcer la sécurité dans un monde de plus en plus incertain.

Que nous dit la recherche au sujet de l'attitude du public à l'égard des risques et de la sécurité ? Les enquêtes menées auprès du public concernant sa perception des divers risques permettent de brosser un portrait complexe et nuancé et font ressortir les grandes différences entre les différentes tranches d'âge, les sexes ainsi que le niveau de richesse et d'éducation[3]. L'utilisation d'un terme générique comme « peur » ne donne qu'un bien mince aperçu de l'éventail complexe de perceptions et d'émotions qu'exprime le public par rapport aux risques. Il est difficile de capter cette façon de penser et de ressentir au moyen de questions fermées et de choix de réponses. Nous devons faire attention de ne pas exagérer l'ampleur des craintes du public. Par exemple, en 2009, 93 % des Canadiens interrogés se disaient satisfaits de leur protection personnelle contre les crimes[4]. Par ailleurs, nous ne voulons pas laisser entendre que le public est toujours passif et tolérant par rapport à ces enjeux. Citons comme exemple le mouvement « Occupy » qui était une réponse directe du public aux risques financiers qui ont mal tourné. Toutefois, cette forme de résistance publique peut devenir une cible pour la surveillance, comme nous l'avons vu lors de la tenue du G20 à Toronto en juin 2010.

En dépit de ces exemples, la psychologie du risque continue d'influencer notre perception des problèmes auxquels nous devons faire face et des solutions qui s'offrent à nous. Les recherches sur la perception du risque ont fait ressortir le « facteur d'appréhension »[5] ; les gens se concentrent sur certains risques improbables en raison de leur nature terrifiante. De la même façon, des recherches psychologiques ont mis en évidence le concept de « disponibilité heuristique »[6], c'est-à-dire la conclusion évidente selon laquelle les risques que nous connaissons le plus deviennent les plus importants pour nous. Prenons par exemple les Américains qui ont été plongés dans une couverture médiatique massive de l'écrasement des avions détournés dans les tours jumelles le 11 septembre 2001. Malgré cet incident terrifiant, l'avion demeure en général plus sûr que la voiture. Or, les événements du 11 septembre ont laissé une si puissante impression que les voyages en avion ont chuté de façon spectaculaire aux États-Unis l'année suivante. Ironiquement, le nombre de voitures sur les routes a augmenté, ce qui a entraîné une nette hausse du nombre de décès sur les routes. Selon le psychologue allemand, Gerd Gigerenzer, il y aurait eu 1 595 décès additionnels aux États-Unis cette année-là[7].

Par ailleurs, les experts et les systèmes experts jouent un rôle clé dans la façon dont nous percevons le risque. Nous nous en remettons souvent aux

experts pour déterminer les risques et nous aider à les gérer. D'un autre côté, les gens estiment de plus en plus que les connaissances des experts ne sont pas particulièrement fiables. Les connaissances de l'expert ne sont jamais définitives et sont en constante évolution. Souvent, les experts ne sont pas du même avis. La population a donc de la difficulté à leur faire confiance. Tout cela vient accentuer le climat de doute et d'anxiété. Par ailleurs, un nombre sans précédent de personnes détiennent un diplôme d'enseignement supérieur, ce qui les rend plus méfiantes et plus critiques. L'Internet nous donne accès à une grande quantité de connaissances alimentant ainsi le climat de doute perpétuel. La confiance du public à l'égard des grandes institutions comme la science, le gouvernement et le marché est minée. Les sondages nous indiquent d'ailleurs un affaiblissement constant de la confiance à l'égard du gouvernement, des politiciens et des autres grandes institutions[8].

De plus, la terminologie qu'utilisent les experts pour parler des risques fait souvent partie du problème. Les experts donnent un sens au risque en l'exprimant au moyen de chiffres et de probabilité, mais au quotidien pour les gens ordinaires, dans les médias et sur la scène politique, la clé réside souvent dans la nature dramatique du risque plutôt que dans sa probabilité. Par définition, les risques dépassent la certitude et le contrôle : un malheur pourrait nous arriver et, même s'il est très peu probable, nous ne pouvons exclure la possibilité qu'il survienne.

De la même façon, il n'est généralement guère utile de parler aux gens des mesures statistiques du risque. Selon les recherches, la plupart des gens auraient tendance à donner un sens au risque, non pas selon les probabilités numériques, mais en fonction de leurs sentiments et de leurs impressions[9]. Des recherches sur la communication des risques réalisées récemment suggèrent également que bon nombre des controverses entourant les risques découlent du fait que les laïques pensent différemment des experts. Autrement dit, les controverses naissent en raison de la différence entre le langage quantitatif des experts et la terminologie qualitative employée couramment par les citoyens dans la vie de tous les jours[10].

Par conséquent, comme le criminologue David Garland, plusieurs théoriciens sociaux soutiennent que le sentiment endémique d'insécurité tend à croître et à être ressenti même par des individus bien nantis qui sont, selon les normes historiques, en meilleure santé et plus riches que jamais. De nos jours, ces gens libérés jouissent de leurs libertés dans un contexte où s'entremêlent une nouvelle dépendance aux systèmes experts et une nouvelle incertitude quant à la vie qu'ils ont choisie[11]. Les gens essaient donc

d'assimiler et de traiter plus de nouveaux renseignements au sujet des risques et se retrouvent parfois submergés.

Notre perception du risque est également influencée par les médias. Depuis toujours, les médias amplifient la nature dramatique des risques. Cependant, la fragmentation du public des médias de masse en créneaux plus spécialisés et polarisés sur le plan politique fait voler en éclats le consensus et alimente la culture d'incertitude et de méfiance. Au Canada, les téléspectateurs de Sun-TV se font dépeindre le monde d'une tout autre façon que ceux de Radio-Canada. De plus, selon les sondages, la confiance à l'égard des médias grand public aurait diminué considérablement[12]. Les médias sociaux comme Facebook et Twitter laissent place à un discours politique critique qui va à l'encontre des vues officielles. Ce discours galvanise son auditoire, certes, mais il accentue l'impression que les certitudes traditionnelles sont ébranlées.

Les grands médias du monde portent souvent notre attention sur des risques improbables, mais terrifiants de sorte qu'ils en accentuent les effets. Les médias de l'information ont ce que les chercheurs appellent une « orientation sur l'événement »[13]. Autrement dit, ils mettent l'accent sur certains événements graves, plutôt que de donner une vue d'ensemble. Bien que les médias aient toujours procédé de cette façon, les nouvelles tendances observées dans les médias du monde avivent les inquiétudes par rapport à certains risques. Par exemple, l'attention portée sur les crimes, particulièrement les crimes violents, a augmenté de façon appréciable au cours des décennies. Dans deux journaux britanniques, cette couverture aurait plus que doublé entre les années 1940 et les années 1990[14]. Dans le cas des informations télévisées, ce phénomène est attribuable en partie à des consultants du secteur, comme Frank N. Magid Associates inc., qui ont commencé dans les années 1980 à conseiller à leurs clients que la couverture médiatique de la criminalité faisait augmenter les cotes d'écoute[15]. Peu importe les motifs, on dresse le portrait d'un monde où les risques prolifèrent en fonction d'événements dramatiques qui choquent et dérangent.

L'élaboration de politiques dans la société du risque

Sous cet angle, la surveillance semble la solution appropriée pour atténuer l'impression généralisée d'insécurité. Les tendances psychologiques, les médias et les politiciens sont autant de facteurs qui contribuent à alimenter

un climat où nombre de mesures de surveillance sont prises pour répondre à un incident qui est dramatique et terrifiant, qui suscite beaucoup l'attention des médias, du public et de la scène politique, mais qui est statistiquement improbable. Le renforcement de la sécurité à la suite des attentats du 11 septembre en est l'exemple le plus frappant. Un autre exemple à l'échelle locale est l'installation petit à petit de caméras de surveillance dans différentes villes canadiennes en raison du tollé suscité par certains crimes violents[16]. Des crimes uniques, mais qui causent de vives impressions, peuvent prendre une importance politique colossale. En 2005, à Toronto, une fusillade survient entre deux gangs au centre-ville de Toronto. Une adolescente de 15 ans, Jane Creba, qui attendait pour profiter des soldes de l'Après-Noël, y perdit la vie. Ce fut un élément décisif qui permit au premier ministre Harper de former son premier gouvernement minoritaire. Selon l'organisateur de sa campagne électorale, Tom Flanagan, les sondages internes avaient déjà établi que la justice pénale était le domaine où les conservateurs avaient le plus d'avance sur les libéraux et la mort tragique de Jane Creba a contribué à bien faire connaître aux électeurs la position du parti dans ce dossier[17]. Bien que ce type d'événement soit extrêmement rare, Stephen Harper a saisi l'occasion pour mener une campagne efficace fondée sur une approche plus dure de lutte contre la criminalité.

Comme nous tolérons de moins en moins le risque, il semble logique de mettre en œuvre des mesures de surveillance à deux fins : recueillir plus de données pour faciliter la détection des risques et offrir une protection contre les délinquants. La nécessité de donner une impression de contrôle prend alors plus d'importance que la nature et la gravité des risques. En 2012, le gouvernement fédéral a notamment adopté un train de mesures de maintien de l'ordre radicales et coûteuses, même si le taux de criminalité, y compris celui des crimes violents, avait atteint son plus bas niveau en 40 ans[18]. Néanmoins, il est *possible* qu'un malheur survienne, même si le risque qu'il nous cause du tort est moins grand qu'auparavant. Comme l'a dit le ministre de la Sécurité publique du Canada devant un comité du Sénat au début de 2012, [traduction] « ne parlons pas des statistiques. Parlons des dangers »[19].

Un exemple qui en dit long au sujet des conséquences sociales est le fait que les politiciens, pour gagner des votes dans certains secteurs stratégiques de l'électorat, peuvent depuis toujours durcir le ton en matière de criminalité, ce qui entraîne une recrudescence des mesures de surveillance. Ainsi, bien que dans les sondages peu de Canadiens expriment une inquiétude par rapport au terrorisme[20], les autorités ont fondé sur la lutte contre le

Surveillance policière lors de la tenue du sommet du G20 au Canada

Dès que le Canada a accepté d'organiser le sommet du G20 à Toronto en 2012, les services de police canadiens ont entrepris l'une des plus vastes opérations nationales de renseignements de l'histoire canadienne. Le Groupe mixte des renseignements dirigé par la GRC comptait 500 employés pendant la période de pointe. Les policiers de la cellule de veille Internet surveillaient intensément les militants dans les médias sociaux dans le cadre d'une enquête de sources ouvertes. Ils ont établi des cartes des réseaux sociaux des militants et ont procédé par inférence pour analyser leur comportement en fonction de leurs abonnements et de leurs abonnés sur Twitter, des événements auxquels ils devaient participer et d'autres renseignements personnels diffusés sur les médias sociaux[1].

Une équipe de douze policiers a infiltré des groupes de manifestants partout au pays. D'ailleurs, deux de ces agents ont prétendu pendant 18 mois être membres d'organisations militantes du sud de l'Ontario. Cette surveillance s'est soldée par le dépôt de 59 accusations criminelles contre 17 personnes, dont la plupart ont été arrêtées de manière préventive dès le premier jour du sommet[2]. Les accusations ont par la suite été abandonnées pour 11 des 17 militants. Les six autres ont plaidé coupable à divers chefs d'accusation mineurs, dont l'encouragement à commettre un méfait. Par ailleurs, des policiers en civils vêtus comme des manifestants se sont mêlés aux manifestants pour filmer avec une douzaine de caméras les manifestations. Enfin, les policiers ont fait appel à une externalisation ouverte (« crowdsourcing ») de la surveillance après le sommet; ils ont notamment publié 40 000 images et 500 vidéos en ligne en demandant au public de les aider à identifier les suspects.

De telles mesures sont un bon exemple de la gestion du risque primant sur les droits. Les policiers ont ciblé les militants parce que, selon eux, ils présentaient un risque pour la sécurité. Au moyen d'une surveillance cachée, ces personnes se sont vu exclues de manifestations démocratiques qui étaient essentiellement pacifiques. Comme la majorité des accusations ont été abandonnées, la reddition de comptes sur le plan juridique, pour la surveillance proprement dite et la liberté d'expression des militants qui a été ainsi brimée, a été évitée, dernière victoire des risques sur les droits.

1. Kate Milberry, « Surveillance and Security Spectacle at the Toronto G20: The Miami Model and the Ambivalence of Social Media », document présenté lors de la conférence *Security and Its Publics*, Université Carleton, Ottawa, 20-22 septembre 2012.
2. Jeff Monaghan et Kevin Walby, « 'They Attacked the City': Security Intelligence, the Sociology of Protest Policing, and the Anarchist Threat at the 2010 Toronto G20 Summit », *Current Sociology* 60, no 5 (2012), p. 653-671.



Une participante prend des photos des policiers pendant les manifestations en marge des sommets du G20/G8 à Toronto le 26 juin 2010 (Source : © iStockphoto.com/Jen Grantham)

terrorisme la vaste campagne de surveillance entourant les manifestations lors des réunions du G20 tenues à Toronto en 2010.

Par ailleurs, de plus en plus de risques sont transférés des gouvernements aux individus et aux entreprises. Les Canadiens font moins confiance au filet de sécurité sociale traditionnel qu'auparavant. Plusieurs sont par exemple de moins en moins sûrs de pouvoir compter sur le Régime de pensions du Canada à leur retraite. Nombreux sont ceux qui se sentent accablés par l'incertitude financière qui accompagne les grandes étapes de l'existence et vivent dans l'incertitude. Les groupes vulnérables, comme les personnes âgées et les personnes pauvres, risquent de devenir de plus en plus marginalisés et privés de droits. Voilà un autre exemple du glissement des droits vers le risque. D'ailleurs, les Canadiens s'inquiètent plus de leurs finances depuis la crise financière de 2008. Plusieurs chercheurs qui étudient l'attitude du public par rapport à la criminalité soutiennent que si les préoccupations sociales et économiques s'accentuent, la population sera plus encline à accepter l'ajout de mesures de lutte contre la criminalité. C'est l'hypothèse du « déplacement »[21] qui, bien que difficile à prouver, pourrait éventuellement nous aider à comprendre les contextes politiques qui permettent l'adoption d'une série de nouvelles mesures de surveillance sans opposition.

Or, ce ne sont pas seulement les risques financiers qui sont transférés aux particuliers dans le processus que les sociologues appellent la « responsabilisation ». Ce processus implique que l'on enjoigne l'individu à surveiller et à prendre en main sa sécurité en milieu de travail, la prévention des actes criminels dont il pourrait être victime ou les habitudes de ses enfants sur Internet – entre autres choses.

Comme le soutient le sociologue Ulrich Beck, dans la société du risque, la hiérarchie sociale repose de plus en plus sur la capacité de gérer le risque plutôt que sur la possession de richesses. Autrement dit, la distinction entre les privilégiés et les démunis se fonde essentiellement non pas sur la répartition des « biens », mais plutôt sur la capacité d'éviter les « maux »[22]. De plus, comme ceux qui sont les plus vulnérables aux risques incluent ceux qui contribuent au risque, certains groupes, comme les minorités ethniques ou les jeunes en difficulté, sont souvent perçus non seulement comme étant à risque, mais également comme étant dangereux. Les personnes marginalisées sont davantage exposées aux risques et sont catégorisées comme de mauvais risques. Par conséquent, ceux qui auraient besoin de notre aide sont paradoxalement vus comme une menace. On insiste sur la menace que représentent ces personnes marginalisées plutôt que sur l'aide dont elles

ont besoin. La société du risque tend alors à devenir, comme le dit le criminologue Jock Young, une « société exclusive »[23] dans laquelle les groupes marginalisés sont exclus des formes souhaitables de sécurité. La fonction de tri social de la surveillance est cruciale dans ce contexte ; la surveillance nous aide à catégoriser et à surveiller les groupes de personnes jugées à risque et, parfois, à les empêcher de participer pleinement à la société.

Il est également important de noter que l'évaluation technique des risques cache souvent des jugements moraux[24]. Le regroupement de citoyens (en particulier ceux qui sont membres de groupes marginalisés) dans des catégories de risque a entraîné une croissance du besoin de connaissances techniques et statistiques. Or, bien que ce processus soit présenté en termes neutres, souvent des évaluations morales – des jugements à propos de qui est bon et de qui est mauvais – se cachent sous la formulation technique des experts. D'ailleurs, les méthodes utilisées pour mesurer le risque sont souvent élaborées et convenues en coulisses ; c'est le cas notamment du développement des algorithmes d'évaluation des risques. Ainsi, comme le travail technique camoufle les jugements de valeurs, ce mode d'évaluation des risques n'est assorti d'aucune obligation de rendre des comptes ; il est donc difficile pour les gens ordinaires de s'y opposer. Encore une fois, le risque peut donc l'emporter sur les droits.

Peu après le 11 septembre, le Canada et les États-Unis ont négocié l'initiative sur la Frontière intelligente. Ce programme est un bon exemple du type de surveillance qui affiche ces caractéristiques[25]. Certains types de voyageurs bénéficient d'un prédédouanement tandis que des algorithmes de cotation des risques sont appliqués pour signaler les catégories de voyageurs pour lesquelles les autorités doivent procéder à d'autres vérifications. La nature exacte des algorithmes et les critères de risques utilisés pour repérer ces personnes demeurent confidentiels. Ce processus de surveillance et de tri social n'est donc assorti d'aucune obligation de rendre compte. Cet exemple est lui aussi révélateur du glissement des droits aux risques.

Le Canada n'a pas été directement touché par les attaques du 11 septembre, mais ces attentats et les incidents terroristes qui se sont produits par la suite à l'étranger ont jeté une ombre qui perdure. D'ailleurs, les suites données aux menaces terroristes ont la qualité de s'autoalimenter : en rappelant au public qu'il y a une menace, les interventions elles-mêmes semblent justifier la nécessité d'accroître la surveillance. Mentionnons par exemple qu'après les attentats de 2005 visant le transport public de Londres en Angleterre, OC Transpo, le fournisseur de service d'autobus d'Ottawa,

a lancé une campagne d'affichage pour accroître la vigilance du public. L'entreprise demandait essentiellement aux usagers de s'espionner entre eux[26]. On pouvait lire sur les affiches « Si vous remarquez quelque chose, dites-le ». Cette mention était accompagnée d'un numéro pour signaler les activités suspectes. En 2006, OC a procédé à une autre campagne d'affichage pour exhorter les usagers à « rapporter tout ce qui peut paraître suspect ». Ces campagnes ne font pas seulement appel aux particuliers pour qu'ils se surveillent entre eux, elles renforcent également l'impression que le danger est toujours présent et justifient ainsi la nécessité d'augmenter la surveillance. Voilà un bon exemple qui illustre comment les efforts pour renforcer la sécurité peuvent parallèlement créer une insécurité.

La surveillance en tant que risque

Dans la société du risque, certains risques sont l'objet d'une attention démesurée pour des raisons politiques, culturelles, médiatiques ou industrielles. Or, il est important de noter qu'il existe également de nouveaux risques qui sont bien réels, sans nécessairement de l'attention qu'ils méritent. La modernisation est une arme à double tranchant : elle permet simultanément d'atténuer certains risques, alors qu'elle en fait jaillir de nouveaux. La surveillance en est un bon exemple. Bien qu'elle soit censée faciliter la gestion des risques, elle en crée de nouveaux pour la protection de la vie privée, l'équité et la liberté. On accorde une place dominante à la science et à la technologie dans la conduite des affaires humaines, en particulier dans la réduction des risques ; pourtant elles sont aussi la source de nouveaux risques, notamment pour ce qui est des changements climatiques, des virus informatiques ou de la fraude par ordinateur. De plus, la rapidité avec laquelle évoluent les technologies fait que nous avons du mal à en suivre le rythme. Les nouvelles technologies, surtout les technologies de l'information, finissent par avoir des conséquences fortuites, tantôt positives, tantôt négatives. La gestion de l'information, que ce soit au nom de l'État, des entreprises ou de tiers, est utile pour faciliter les déplacements, le divertissement, les communications, la production industrielle et d'autres opérations économiques, mais elle soulève aussi des préoccupations quant à la surveillance et à la protection de la vie privée. Les percées dans le domaine des caméras de surveillance, de la biométrie, de la génétique, des systèmes de localisation et de poursuite, de la miniaturisation et de la convergence

entre les ordinateurs et les systèmes de télécommunication ont fait de la collecte, du stockage, de la récupération et du traitement de l'information une partie centrale de la vie, comme jamais auparavant. De plus, la réglementation accuse souvent un retard par rapport au déploiement de ces nouvelles technologies.

L'augmentation vertigineuse des innovations technologiques et de leur propagation est particulièrement visible dans le monde de l'informatique et d'Internet, lesquels ont connu une croissance qui nous laisse souvent perplexe. À titre d'exemple, au cours d'une période de deux ans le nombre d'appareils électroniques (des ordinateurs aux téléphones intelligents) connectés à Internet passait de 20 000 à 80 000 au cours des années 1980 et de 20 millions à 80 millions la décenne suivante[27]. Selon un article paru dans *The Economist,* une estimation aurait établi que l'humanité a créé 150 milliards de gigaoctets de données en 2005 et qu'elle en aura créé 1 200 milliards de gigaoctets en 2010[28]. Un sondage d'opinion mené en 2009 a indiqué que les Canadiens s'inquiétaient à peine des risques pour la protection de la vie privée que pouvaient présenter les technologies de réseautage en ligne. Deux ans plus tard, près de 51 % des Canadiens affirmaient s'inquiéter de la menace pour la vie privée que représentent les médias sociaux comme Facebook et Twitter[29]. Les risques d'atteinte à la vie privée découlant des médias sociaux sont un bon exemple de risques technologiques évoluant à un rythme que nous avons du mal à suivre.

Conclusion

En comprenant la tendance relative vers la « sécurité », nous pouvons mieux saisir le grand contexte social dans lequel les nouvelles mesures de surveillance continuent de voir le jour au Canada. De plus, nous pouvons analyser certains des facteurs qui facilitent l'adhésion à ces mesures ou qui rendent plus difficile leur contestation. Il est toutefois encourageant de constater que, dans l'ensemble, la population canadienne est plus instruite et mieux informée, plus méfiante et plus critique à l'égard de différentes autorités et des institutions en général qu'auparavant. Si cette tendance accroît le sentiment d'incertitude et d'insécurité des Canadiens, elle peut également favoriser une certaine remise en question : quand la gestion du risque, la sécurité et la surveillance deviennent-elles excessives ? Quelles sont les meilleures façons de trouver un équilibre entre les risques et les droits ?

Notes

1 Voir Dan Gardner, *Risk: Why We Fear the Things We Shouldn't—and Put Ourselves in Greater Danger* (Toronto, McClelland and Stewart, 2008).

2 Voir Ulrich Beck, *World at Risk* (Cambridge, Royaume-Uni, Polity Press, 2009) ; Anthony Giddens, *Runaway World: How Globalization Is Reshaping Our Lives* (Londres et New York, Routledge, 2003), chapitre 2 ; et Anthony Giddens, *Modernity and Self-Identity* (Cambridge, Royaume-Uni, Polity Press, 1991).

3 Peter Taylor-Gooby et Andreas Cebulla, « The Risk Society Hypotheses: An Empirical Test Using Longitudinal Survey Data », *Journal of Risk Research* 13, nº 6 (2010), p. 731-752.

4 Shannon Brennan, *Les perceptions des Canadiens à l'égard de la sécurité personnelle et de la criminalité, 2009,* Statistique Canada (Ottawa, Ministère de l'Industrie, 2011), http://www.statcan.gc.ca/pub/85-002-x/2011001/article/11577-fra.htm, p. 5.

5 Paul Slovic, Baruch Fischhoff et Sarah Lichtenstein, « Why Study Risk Perception ? », *Risk Analysis* 2, nº 2 (1982), p. 83–93.

6 Amos Tversky et Daniel Kahneman, « Judgment Under Uncertainty: Heuristics and Biases », *Science* 185, nº 4157 (septembre 1974), p. 1124–1131.

7 Cité dans Gardner, *Risk,* p. 4.

8 Voir, par exemple, Edelman Trust Barometer, Étude mondiale annuelle 2012, http://trust.edelman.com/trusts/trust-in-institutions-2/.

9 Brian Wynne, « May the Sheep Safely Graze ? A Reflexive View of the Expert–Lay Knowledge Divide », dans Scott Lash, Bronislaw Szerszynski et Brian Wynne (dir.), *Risk, Environment, Modernity: Towards a New Ecology* (Londres, Sage, 1996) p. 27–43.

10 William Leiss et Douglas Powell, *Mad Cows and Mother's Milk: The Perils of Poor Risk Communication,* 2e éd. (Montréal et Kingston, McGill-Queen's University Press, 2004), p. 27-28.

11 David Garland, « The Rise of Risk », dans Richard V. Ericson et Aaron Doyle (dir.), *Risk and Morality* (Toronto, University of Toronto Press, 2003), p. 78.

12 Pew Research Centre, « Press Accuracy Rating Hits Two Decade Low », Public Evaluations of the News Media, 1985-2009, 13 septembre 2009, http://www.people-press.org/2009/09/13/press-accuracy-rating-hits-two-decade-low/.

13 Richard Ericson, Patricia Baranek et Janet Chan, *Visualizing Deviance: A Study of News Organization* (Toronto, University of Toronto Press / Milton Keynes, Royaume-Uni, Open University Press, 1987).

14 Robert Reiner, Sonia Livingstone et Jessica Allen, « No More Happy Endings ? The Media and Popular Concern About Crime Since the Second World War », dans Tim Hope et Richard Sparks (dir.), *Crime, Risk and Insecurity: Law and Order in Everyday Life and Political Discourse* (Londres et New York, Routledge, 2001), p. 13-32.

15 Margalit Fox, « Frank Magid, Creator of 'Action News,' Dies at 78 », *New York Times,* 9 février 2010.

16 Emily Smith, « The Piecemeal Development of Camera Surveillance in Canada », dans Aaron Doyle, Randy Lippert et David Lyon (dir.), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Londres et New York, Routledge, 2012), p. 122-135.

17 Tom Flanagan, *Harper's Team: Behind the Scenes in the Conservative Rise to Power,* 2e éd. (Montréal et Kingston, McGill-Queen's University Press, 2009), p. 247.

18 Voir Shannon Brennan, *Statistiques sur les crimes déclarés par la police au Canada, 2011*, Statistique Canada (Ottawa, Ministère de l'Industrie, 2012), http://www.statcan.gc.ca/pub/85-002-x/2012001/article/11692-fra.htm, p. 6.

19 Voir Meagan Fitzpatrick, « Omnibus Crime Bill Hearings Underway in Senate », *CBC News*, 1er février 2012, http://www.cbc.ca/news/politics/omnibus-crime-bill-hearings-underway-in-senate-1.1298713.

20 Concernant l'étendue des préoccupations quant au terrorisme des Canadiens, voir Louise Lemyre, Michelle C. Turner, Jennifer E. C. Lee et Daniel Krewski, « Public Perception of Terrorism Threats and Related Information Sources in Canada: Implications for the Management of Terrorism Risks », *Journal of Risk Research* 9, no 7 (2006), p. 755-774.

21 Stuart A. Scheingold, « Politics, Public Policy and Street Crime », *Annals of the American Academy of Political and Social Science* 539 (mai 1995), p. 155-168.

22 Voir Ulrich Beck, *Risk Society: Towards a New Modernity,* traduit en anglais par Mark Ritter (Londres, Sage Publications, 1992), et, pour une analyse de l'argument de Beck sur les classes, voir Dean Curran, « Risk Society and the Distribution of Bads: Theorizing Class in the Risk Society », *British Journal of Sociology* 64, no 1 (2013), p. 44–62.

23 Jock Stuart Young, *The Exclusive Society* (Beverly Hills, CA, Sage, 1999).

24 Richard V. Ericson et Aaron Doyle, « Risk and Morality », dans Ericson et Doyle (dir.), *Risk and Morality*, p. 1-10.

25 Mark B. Salter, « Citizenship, Borders and Mobility: Managing Canada's Population », dans Claire Turenne Sjolander et Heather Smith (dir.), *Canada in the World: Internationalism in Canadian Foreign Policy* (New York, Oxford University Press, 2013), p. 146-163.

26 Mike Larsen et Justin Piche, « Public Vigilance Campaigns and Participatory Surveillance After 11 September 2001 », dans Sean P. Hier et Joshua Greenberg (dir.), *Surveillance: Power, Problems, and Politics* (Vancouver, University of British Columbia Press, 2010), p. 187-202.

27 Ray Kurzweil, « The Law of Accelerating Returns, » 7 mars 2001, www.kurzweilai.net/the-law-of-accelerating-returns.

28 « The Data Deluge », *The Economist,* 25 février 2010, http://www.economist.com/node/15579717.

29 Harris/Decima, *Sondage sur les Canadiens et la protection de la vie privée, 2011*, présenté au Commissariat à la protection de la vie privée du Canada, Ottawa, 31 mars 2011, https://www.priv.gc.ca/information/por-rop/2011/por_2011_01_f.asp.



Décloisonnement des secteurs

Le public et le privé, d'opposition à combinaison

Tout au long de notre vie nous fournissons, dans une série de contextes différents, des renseignements personnels au secteur public et au secteur privé. Lorsque nous produisons une déclaration de revenus ou que nous demandons un permis de conduire, nous savons que l'information que nous fournissons sera conservée par le gouvernement dans un dossier. De la même façon, lorsque nous utilisons notre carte de crédit, que nous signons un contrat de téléphonie ou que nous adhérons à un programme de fidélisation de la clientèle, nous savons que la société avec laquelle nous faisons affaire conservera un registre de nos contacts avec elle et de ce que nous lui disons. Si nous nous préoccupons de la collecte et de l'utilisation de cette information, ces préoccupations tendent à varier selon que nous ayons affaire à un gouvernement ou à une entreprise privée. D'ailleurs, au Canada, les dispositions législatives sur la protection des renseignements personnels qui s'appliquent aux organismes publics et aux entreprises ne sont pas les mêmes.

Les lois sur la protection des renseignements personnels visant le secteur public visent notamment à éviter la création d'un *Big Brother*. Comme il peut être plus difficile pour les citoyens de jouir des libertés démocratiques en raison de la surveillance exercée par le gouvernement, nous nous attendons habituellement à ce qu'il obtienne un mandat avant d'entrer dans nos maisons et d'envahir notre vie privée. D'une part, nous nous attendons également à ce que les organismes gouvernementaux ne recueillent que les

données personnelles qui sont requises pour réaliser des objectifs législatifs et n'utilisent et ne divulguent ces données qu'à des fins concordant avec ces objectifs. D'autre part, les lois limitant la collecte d'information dans le secteur privé portent sur des enjeux relatifs à la consommation, notamment sur les façons de corriger les erreurs relatives aux cotes de solvabilité ou sur les renseignements que les responsables-marketing peuvent recueillir sans notre consentement. Pendant presque tout le XXe siècle, nous pouvions raisonnablement supposer que, en l'absence de mandat en bonne et due forme, l'information que nous fournissions au gouvernement et celle que nous fournissions aux entreprises étaient cloisonnées.

Or, ce n'est plus le cas. Bien qu'il existe des limites techniques, organisationnelles et juridiques à la circulation des renseignements, il est manifeste que les données circulent maintenant librement entre les organismes publics et les sociétés privées. En effet, les données d'un secteur se retrouvent si souvent dans un autre secteur qu'il est maintenant difficile de faire la distinction entre la surveillance faite par le gouvernement et celle faite par le secteur privé. Cependant, comme les gouvernements et les entreprises ont des motivations et des mandats très différents, les implications en matière de redevabilité sont énormes.

Prenons l'exemple du Service canadien du renseignement de sécurité (SCRS), qui est l'organisme responsable de notre protection contre les menaces provenant de l'étranger. Le SCRS explore activement les possibilités de partenariats avec des propriétaires et exploitants du secteur privé qui lui permettraient de demander aux entreprises de lui fournir des renseignements personnels au sujet de leurs clients, et ce, sans le consentement des clients. L'objectif du SCRS est de bâtir un réseau de contacts régionaux, ou à proprement parler une toile de surveillance, avec les propriétaires et exploitants d'entreprises qui sont considérées comme des infrastructures essentielles. La toile ainsi tissée irait des pipelines aux sables bitumineux en passant par le transport public[1].

Une fois que le secteur privé achemine ces données au gouvernement, il devient très difficile pour la population de faire le suivi, voire de contrôler, ses renseignements personnels. Comment pouvez-vous savoir si le SCRS a monté un dossier sur vous à partir d'information glanée auprès des sociétés de transport en commun ou de l'entreprise du secteur de l'électricité pour laquelle vous travaillez ? Qui plus est, comme les préoccupations relatives aux technologies et à la sécurité favorisent le décloisonnement des secteurs public et privé, comment pouvez-vous déterminer qui est responsable si

vous subissez un préjudice et à quelle instance vous adresser pour obtenir de l'aide ?

Le décloisonnement des secteurs publics et privés est lui-même provoqué par deux grands facteurs. Tout d'abord, l'idée répandue selon laquelle le gouvernement et le secteur privé devraient travailler en tandem afin d'optimiser l'efficacité et la productivité. Par conséquent, nombre de tâches qui étaient autrefois effectuées par le gouvernement sont maintenant confiées à des entreprises. À titre d'exemple, l'analyse des données du recensement du Canada a été confiée à Lockheed Martin, qui utilise son propre logiciel et matériel de traitement des données, et le gouvernement de la Colombie-Britannique a retenu les services de l'entreprise américaine Maximus pour l'exécution de son régime de services médicaux et de son assurance-médicaments (Pharmacare). Ensuite, les nouvelles technologies favorisent la rupture des frontières traditionnelles entre les institutions parmi les secteurs et à l'intérieur de ceux-ci. Les données peuvent ainsi circuler dans les deux directions sans qu'un mandat judiciaire ne soit requis. Par conséquent, on peut affirmer que le décloisonnement des secteurs publics et privés est à la fois une cause et une conséquence de l'augmentation de la surveillance.

Les tendances sont complexes et nombreuses ; pour les mettre en évidence, nous nous concentrerons sur trois nouvelles pratiques qui ont estompé le cloisonnement institutionnel entre les organismes publics et privés : l'accès aux données sur les communications par les organes d'application de la loi ; les modifications législatives qui nécessitent un partage sans cesse plus grand de données personnelles entre les entreprises et le gouvernement et vice versa ; et la sous-traitance de fonctions de sécurité à « l'industrie de la surveillance ».

Qu'est-ce qui a suscité la collaboration public-privé ?

À partir des années 1980, à l'instar d'autres gouvernements étrangers, le Canada a commencé à réduire la taille du secteur public, à privatiser certains services gouvernementaux, à permettre la création et l'expansion de services de sécurité privée et de maintien de l'ordre, et à réduire les programmes de soins de santé, d'éducation et de pensions. Comme les services financés par le public ont été réduits, ceux qui en ont les moyens se sont tournés vers le secteur privé pour les acheter. Par conséquent, nous devenons tous de plus

en plus tributaires d'entreprises et de corporations pour la prestation des services communautaires dont nous avons besoin.

Cependant, contrairement aux gouvernements, les entreprises ont tendance à croire que les renseignements personnels qu'elles recueillent dans le cadre de la prestation de ces services constituent un actif précieux dont elles peuvent se servir pour générer des profits. Il s'agit là d'un facteur important qui les incite à obtenir et à conserver de plus en plus de données sur les citoyens. Conformément au cadre juridique, les entreprises sont tenues d'obtenir le consentement des particuliers pour recueillir ces données. Néanmoins, comme les services commerciaux deviennent de plus en plus nécessaires dans notre vie quotidienne, nous devons choisir entre deux options : soit nous consentons à ce que notre information soit achetée et vendue, soit nous renonçons aux avantages associés aux commodités que sont l'utilisation d'une carte de crédit, l'obtention d'un prêt hypothècaire ou le recours à des traitements de physiothérapie. D'ailleurs, nous nous trouvons devant un dilemme semblable dans le contexte de la sécurité : soit nous consentons à faire vérifier nos bagages et nos communications, nous enlevons nos souliers, nous fournissons nos empreintes digitales et nous subissons à l'occasion des fouilles corporelles, soit on nous interdit de prendre l'avion.

Une fois ces données personnelles recueillies, elles peuvent facilement passer des mains des sociétés à celles du gouvernement. Les renseignements commerciaux à notre sujet sont notamment recueillis puis revendus par des courtiers en données (privés) à des organismes (publics) comme le SCRS et les services de police[2]. Bien entendu, un organe comme l'Agence des services frontaliers du Canada (public) a couramment accès aux renseignements sur les passagers que les transporteurs aériens (privés) sont obligés de lui transmettre avant qu'un avion ne décolle. À l'inverse, certains renseignements gouvernementaux au sujet des citoyens sont filtrés par des entités commerciales. Prenons par exemple Postes Canada qui vend de l'information sur les « changements d'adresse » à des responsables-marketing (privés). D'ailleurs, le système des codes postaux est largement utilisé par les spécialistes du marketing pour catégoriser les consommateurs.

Alors que l'information commence à circuler plus librement entre les secteurs publics et privés, l'infrastructure qui détermine les pratiques organisationnelles a changé. Les dossiers constitués manuellement et rangés dans un classeur ou les réunions en personne ou au téléphone sont maintenant remplacés respectivement par des bases de données informatiques et

des plateformes de communications en réseau. Les métaphores mécaniques qui régnaient autrefois dans le monde des documents papier, des classeurs et des téléphones, ont été remplacées par l'image de données électroniques filant comme l'éclair dans une galaxie électronique.

Au fil du temps, les gains d'efficacité attribués aux nouvelles technologies ont été accompagnés d'une transformation des pratiques organisationnelles. Le nouveau modèle industriel de la « gestion de la relation-client » et le marketing par bases de données sont fondés sur l'analyse du consommateur, dont les préférences et les habitudes de consommation sont suivies et stockées dans des systèmes informatiques. De nouveaux logiciels ont changé les moyens utilisés par les entreprises pour obtenir des données directement à partir des achats des consommateurs. Parallèlement, les entreprises ayant recours à ces techniques ont commencé à offrir des avantages et des récompenses aux consommateurs, en échange de leurs renseignements personnels.

L'information en soi est devenue fondamentale, et donc précieuse : elle peut être utilisée non seulement par les entreprises qui ont mis en œuvre le système, mais également par des tiers s'intéressant aux habitudes de consommation de groupes et de particuliers. Parmi ces tiers, citons les courtiers en données mentionnés précédemment, qui font le commerce des données personnelles. De cette façon, grâce aux nouvelles technologies, on a ouvert les écluses à une circulation sans précédent de données personnelles, au sein des organismes et entre ceux-ci. Comme le montrent les exemples suivants, ce n'était qu'une question de temps avant que les barrières conventionnelles entre public et privé ne s'effritent et permettent d'abord les fuites, puis un flot de données des gouvernements aux entreprises et à l'inverse.

Accès aux communications privées par les organes d'application de la loi

L'exemple suivant est l'un des plus éloquents et des plus controversés des conséquences de cette libre circulation des données entre les secteurs public et privé. Il touche les dispositions sur « l'accès légal » qui visent à faciliter l'accès des policiers aux données générées par les utilisateurs de systèmes de réseaux de communication.

En 2011, le projet de loi omnibus contre la criminalité, regroupant trois projets de loi, était déposé au Parlement canadien. Selon les articles dignes d'intérêt, les fournisseurs d'accès Internet (FAI) étaient obligés de

fournir à la police des données sur certains abonnés (l'identité d'une personne utilisant une certaine adresse IP)* pour des raisons de « sécurité », sans qu'un mandat ne soit requis. Les commissaires à la protection de la vie privée tant fédéral que provinciaux firent état de préoccupations majeures concernant le projet de loi qui, dans les faits, donnait une fonction de police aux FAI. Ils envoyèrent au ministre de la Sécurité publique du Canada une lettre conjointe dans laquelle étaient regroupées leurs préoccupations. Parallèlement, une campagne médiatique à la télévision et sur Internet appelée « Arrêter l'espionnage en ligne » vit le jour, visant à sensibiliser la population aux conséquences négatives considérables de l'adoption d'une telle loi ; 145 000 Canadiens signèrent la pétition en ligne pour exprimer leurs inquiétudes. Par conséquent le projet de loi fut mis en veilleuse et, plusieurs mois après la débâcle, le gouvernement annonçait qu'il abandonnait le dossier. Néanmoins, il serait prématuré de conclure que la question est définitivement réglée. En effet, il est prouvé que la plupart des fournisseurs acheminent déjà des données personnelles aux policiers, sans qu'un mandat ne soit émis ou qu'ils soient tenus de le faire en vertu de dispositions législatives[3].

Le projet de loi demeure un excellent exemple des conséquences du décloisonnement des secteurs publics et privés et de l'admission des entreprises privées dans les affaires du gouvernement. Entrant dans la suite logique de l'efficacité et de la privatisation, la nouvelle loi aurait obligé les fournisseurs d'accès Internet à modifier leurs systèmes pour qu'ils prennent en charge la surveillance en temps réel. De plus, les nouveaux pouvoirs conférés aux policiers les auraient habilités à obtenir l'accès à des données générées alors que les gens vaqueraient à leurs occupations quotidiennes en ligne (magasiner, travailler, naviguer sur les médias sociaux), et ce, que l'utilisateur le fasse de façon anonyme ou non. Cela, sans la supervision nécessaire pour éviter que l'on n'abuse de ces pouvoirs. L'une des dispositions qui posaient particulièrement problème aurait permis aux policiers de contraindre un FAI à identifier un utilisateur anonyme sur Internet, *et ce, même si on doutait que cela soit utile pour une enquête.* Comme le projet de loi imposait aux FAI des interdictions catégoriques de divulguer les demandes de surveillance faites par les policiers, on dissimulait encore plus la façon dont les vastes pouvoirs

* L'adresse IP est un numéro attribué à chaque appareil (ordinateur, imprimante, etc.) qui fait partie d'un réseau informatique connecté à Internet.

accordés auraient été utilisés, ce qui aurait rendu encore plus difficile de contester un abus de ces pouvoirs devant les tribunaux.

Les critiques soutenaient que si le projet de loi était adopté, les citoyens canadiens, les fournisseurs d'accès Internet, les réseaux sociaux et même les téléphones et les voitures pourraient servir d'outils d'espionnage pour l'État. Bien que le projet de loi n'ait pas été voté, son dépôt prouve clairement comment la tendance au décloisonnement entre le public et le privé bouleverse les attentes consacrées quant au type de relations que les citoyens entretiennent avec leur gouvernement dans une démocratie.

Ces conflits législatifs révèlent également la mesure dans laquelle les entreprises privées sont perçues comme des outils essentiels pour les organes d'application de la loi. À titre d'exemple, l'entreprise Google (comme Twitter et quelques autres) indique périodiquement le nombre de demandes de renseignements qu'elle reçoit de la police au sujet de ses utilisateurs, pour chaque pays. Sans surprise, alors que le nombre d'utilisateurs de Google augmente, le nombre de demandes connaît aussi une nette hausse[4]. Google accède à environ 24 % des demandes canadiennes, tandis que Twitter n'acquiesce qu'à 7 % d'entre elles. Cependant, il existe d'importantes disparités nationales et peu d'information au sujet des types de demandes reçues. Plusieurs entreprises en ligne ont exercé de fortes pressions pour que des normes juridiques claires et uniformes soient adoptées. Ces normes leur permettraient de connaître les conditions conformément auxquelles ces demandes doivent être acceptées ou refusées. Google fait toutefois preuve d'une relative transparence dans ce dossier, contrairement à la plupart des entreprises. Il est à noter néanmoins que des entreprises canadiennes comme Distributel et TekSavvy s'opposent carrément à l'accès sans mandat aux données des utilisateurs. Les petits fournisseurs d'accès Internet, qui ne disposent pas d'importantes ressources juridiques, pourraient par contre avoir plus de mal à refuser les demandes de données.

Il est encore plus inquiétant de constater la quantité de données qui sont échangées par des moyens détournés. En 2005, cette question a provoqué un grand retentissement dans les médias, alors qu'un dénonciateur faisait parvenir à la Electronic Frontier Foundation des preuves selon lesquelles l'entreprise AT&T avait laissé installer un diviseur optique à son centre de San Francisco. La National Security Agency (NSA) des États-Unis utilisait ce dispositif pour surveiller en temps réel les courriels et la navigation sur le Web de tous les clients d'AT&T (se reporter aux Tendances 6 et 7)[5]. Cette révélation a rapidement entraîné de nombreuses poursuites

en justice contre AT&T. Ces poursuites ont toutefois été arrêtées lorsque le Congrès est intervenu en modifiant le *Foreign Intelligence Security Act* en vue de dégager les « fournisseurs de services de communication électronique » comme AT&T de toutes responsabilités lorsqu'ils coopèrent avec les services de renseignements. Les modifications à la loi ont également entraîné l'imposition de sanctions aux entreprises qui contreviennent à une ordonnance émise en vertu de la loi ou même qui rendent publique l'existence de cette ordonnance. La loi a été renouvelée en janvier 2013 et demeurera en vigueur au moins jusqu'en 2018. Bien entendu, la dénonciation d'Edward Snowden à l'été 2013 a ravivé le débat sur les liens en matière de surveillance existants entre la NSA, des entreprises privées et l'information personnelle recueillie auprès de citoyens ordinaires tant aux États-Unis que dans d'autres pays, comme le Canada.

Parmi les modifications apportées au *Foreign Intelligence Security Act*, citons l'ajout des termes « remote computing services » (service de traitement à distance) ou « cloud computing » (informatique en nuage) à la définition actuelle de « electronic communication service provider » (fournisseurs de services de communication électronique). Selon un rapport récemment déposé au Parlement européen, ces modifications ont permis aux organismes américains d'avoir accès aux dossiers des consommateurs et à d'autres renseignements à partir de divers centres informatiques infonuagiques appartenant à des entreprises étatsuniennes et situés aux États-Unis, en Europe ou dans d'autres pays, dont le Canada[6]. Par ailleurs, l'une des dispositions de grande portée de la loi permet de cibler des organisations politiques étrangères ou des territoires à l'étranger qui auraient des liens avec la conduite des affaires étrangères des États-Unis[7]. De plus, les organismes non gouvernementaux canadiens qui pourraient faire appel aux services d'infonuagique d'entreprises comme Google, Microsoft, Amazon et Apple pour stocker des courriels et des données n'échappent pas à ces dispositions. Sans compter que les lois canadiennes sur la protection de la vie privée ne s'appliquent pas aux activités de renseignement des organismes étatsuniens[8].

Le désir des organes d'application de la loi d'accéder aux données sur les communications est un facteur de première importance de la tendance relative au décloisonnement entre les organismes publics et privés. En effet, on observe que dans nombre d'autres pays, les gouvernements se sont déjà engagés dans cette voie. On ne s'attend donc pas à ce que cette question soit reléguée aux oubliettes bientôt ou si aisément. Force est de constater

que, même sans l'adoption de lois en bonne et due forme ou même si le public est résolument opposé à cette distribution incontrôlée de ses données, il est possible que ces pratiques soient appliquées en secret, à l'abri du contrôle démocratique. Le décloisonnement entre les organismes du secteur public et du secteur privé sur le plan des données personnelles est également révélateur de la croissance de la surveillance, une surveillance qui est de plus en plus difficile à détecter et à vérifier. Le prochain exemple montre également comment les données privées sont utilisées à des fins publiques.

Données privées utilisées à des fins publiques et inversement

On conçoit aisément que des organismes de sécurité, comme le SCRS ou le Service de sécurité de la Gendarmerie royale du Canada (GRC), soient chargés d'être à l'affût d'activités telles que le terrorisme et le blanchiment d'argent. Cependant, ces tâches sont également confiées à des entreprises, comme des banques, qui embauchent du personnel pour l'analyse de données et pour d'autres fonctions connexes en vue de détecter les cas suspects et de remettre l'information pertinente aux autorités reconnues. Comme nous l'avons démontré, les données recueillies par les gouvernements à des fins publiques sont de plus en plus transmises au secteur privé. À l'inverse, les données recueillies par des sociétés dans le cadre d'activités commerciales sont communiquées aux gouvernements. Enfin, beaucoup de ces échanges sont autorisés par la loi et font donc l'objet d'une certaine surveillance.

Le Centre d'analyse des opérations et déclarations financières du Canada, le CANAFE, en est un excellent exemple. Ce Centre a pour mandat, au titre de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* de 2000, de « recueillir des renseignements sur les opérations financières et de les analyser, et de communiquer de l'information stratégique afin de faciliter la détection, la prévention et la dissuasion du blanchiment d'argent et du financement des activités terroristes »[9]. Toute entité financière, soit toutes les banques, les caisses populaires et les compagnies d'assurance-vie, de même que tous les courtiers en valeurs mobilières, les conseillers en placement, les courtiers de change, les promoteurs immobiliers, les exploitants de casinos et, même, les marchands de métaux précieux, sont tenus par la *Loi* de déclarer au CANAFE les détails de toutes leurs transactions au comptant d'une valeur supérieure à 10 000 dollars. Le consentement de la personne à qui l'information « appartient » *n'est pas requis*. Au titre d'un protocole d'entente, l'information déclarée au CANAFE



Types de renseignements personnels (Source : © iStockphoto.com/Danil Melekhin)

est ensuite communiquée à la GRC, au Centre d'information de la police canadienne et à d'autres organes similaires.

Le système du CANAFE a pu être matérialisé grâce à l'évolution des technologies informatiques qui sont venues changer la façon dont le secteur privé gère ses finances. Les Bourses dans le monde entier jouent un rôle crucial au pays, parce qu'elles créent le marché sur lequel les produits financiers (et d'autres produits) sont négociés et sur lequel l'offre et la demande (en théorie) déterminent la valeur et fixent le prix. Reste que nous pouvons observer ici aussi les usages novateurs des masses de données : les décisions commerciales sont maintenant robotisées et les ordres d'achat et de vente sont produits par de puissants ordinateurs selon des algorithmes commerciaux que les fonds spéculatifs et les banques d'investissement ont programmés. La tenue des dossiers est informatisée et les échanges sont faits de jour comme de nuit. Force est de constater que les ordinateurs sont plus rapides que les humains ; les plateformes de négociation électronique ont donc

permis de réduire le temps requis pour effectuer une transaction à quelques millisecondes, de sorte que le volume des échanges a augmenté en flèche[10].

Les échanges se produisent à une telle vitesse, la programmation est si perfectionnée et les ordinateurs si puissants que la prévention de la fraude ne peut être qualifiée que de défi colossal pour les chiens de garde du gouvernement qui réglementent le marché. Or, contrairement au SCRS et à la GRC, ces chiens de garde ne sont pas investis de pouvoirs ni ne disposent d'outils ou du consentement des gouvernements pour poursuivre les transgresseurs. Ils doivent plutôt demander aux institutions financières d'avoir recours à leur propre système de surveillance en temps réel pour surveiller les transactions sur les marchés boursiers et pour signaler aux responsables les transactions qui semblent anormales. De cette façon, les fonctions de surveillance policière sont sous-traitées au secteur privé, le même secteur qui mène ces activités commerciales.

Les dossiers des passagers (*passenger name records*), qui sont créés chaque fois qu'un billet d'avion est réservé, constituent également une mine de données commerciales dont les gouvernements peuvent se servir pour faire de la surveillance. Ces dossiers sont traités dans de vastes systèmes mondiaux de distribution ; le principal utilisé au Canada est le système Galileo, implanté au Colorado. Ils peuvent révéler une grande quantité de renseignements délicats sur les préférences des voyageurs, notamment sur les exigences pour les repas, les handicaps, les pratiques religieuses et les allergies. Les transporteurs aériens recueillent également des données sur les réfugiés et les personnes expulsées ; ces données sont utilisées en vue de dresser les listes des personnes interdites de vol par les programmes de précontrôle des passagers, comme la « Secure Flight » de la Transportation Security Administration aux États-Unis et son pendant canadien le programme « Protection des passagers »[11]. L'échange de données provenant des dossiers des passagers entre les pays attise continuellement les tensions et relance sans cesse les négociations entre les agences européennes de protection des données et les autorités étatsuniennes.

Des données sur les citoyens canadiens sont également diffusées largement à nos partis politiques. En vertu de la *Loi électorale du Canada*, Élections Canada est autorisé à communiquer les données de base de la liste électorale. Les règles concernant ce type de divulgation sont présentées assez rigoureusement dans la *Loi*. Néanmoins, chacun des grands partis fédéraux utilise l'information provenant de la liste électorale pour constituer de plus vastes « bases de données de gestion de l'électorat ». Ces bases de

Les exigences des systèmes de sécurité peuvent violer les principes de la dignité et de la présomption d'innocence

Le raisonnement derrière des systèmes comme celui du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) est qu'une meilleure circulation de l'information entre le secteur privé et le secteur public permettra à l'État de détecter les activités illicites, comme le blanchiment d'argent ou le terrorisme, et de poursuivre en justice leur auteur. Or, ce type de surveillance peut créer un réel préjudice pour les personnes qui sont identifiées par erreur comme « suspectes ».

À titre d'exemple, un étudiant canadien qui étudie au Royaume-Uni peut déclencher une enquête simplement en déposant une bourse dans un compte bancaire britannique. Une augmentation soudaine et considérable du montant d'argent dans un compte, surtout si le compte est nouveau, est un élément qui peut signifier une activité illicite et déclencher une enquête criminelle. De plus, certaines universités britanniques qui détiennent un permis pour recruter des étudiants étrangers au moyen d'un régime d'immigration basé sur un système de pointage doivent faire un suivi de l'assiduité de ces étudiants; un étudiant étranger qui manque un cours

données contiennent également une série d'autres données sur les électeurs qui proviennent de diverses sources du secteur privé : sondage téléphonique, techniques conventionnelles de démarchage, pétitions, lettres, bases de données géodémographiques et bases de données de commercialisation offertes sur le marché et analyse des comportements en ligne, dont dans les médias sociaux. Toutefois, ces bases de données soulèvent une controverse de plus en plus vive : premièrement, elles peuvent avoir une incidence considérable sur le processus démocratique et deuxièmement, elles ne sont réglementées par aucune des dispositions législatives sur la protection des renseignements personnels[12].

Par ailleurs, les données dites publiques sont largement utilisées à des fins privées. Bien que la majorité de ces données soient générées de manière agrégée ou générique (par exemple, « 64 % des Canadiens paient le solde de leur carte de crédit en entier tous les mois »), une partie d'entre elles se rapporte à des individus. À titre d'exemple, les entreprises d'évaluation de la solvabilité, comme Equifax, utilisent de l'information publique pour évaluer votre cote de solvabilité et ainsi déterminer si vous faites partie des « bons »

peut avoir des démêlés avec la justice. Si l'étudiant manque dix entretiens consécutifs sans en avoir la permission, l'université peut le signaler aux autorités.

L'University of East London va quant à elle un peu plus loin : les étudiants étrangers qui manquent 25 % de leurs cours sont automatiquement radiés. D'autres écoles demandent aux étudiants étrangers de se présenter en personne au personnel pour un contrôle. À la Coventry University, les étudiants étrangers doivent présenter leur carte d'identité à des postes de surveillance désignés au moins trois fois par semaine. Tant l'University of Greenwich que l'University of the West of England obligent les étudiants étrangers à se présenter une fois par mois. La Fédération des étudiantes et étudiants du Royaume-Uni s'est opposée à ce type de surveillance; elle soutient que les contrôles en personne sont discriminatoires et qu'ils violent la dignité des étudiants étrangers. Elle craint également que ce genre de pratiques minent la relation de confiance qui est au cœur de la vie universitaire[1].

1. Daniel Stevens, « Attendance Monitoring Has Gone Too Far—NUS Pulls Out the Stop Sign », billet d'invité, Joint Council for the Welfare of Immigrants, 14 novembre 2012, http://www.jcwi.org.uk/blog/2012/11/14/attendance-monitoring-has-gone-too-far-%E2%80%93-nus-pulls-out-stop-sign#sthash.g1ejytLm.dpuf.

ou des « mauvais » risques de crédit. Ces entreprises doivent avoir accès à de nombreux dossiers publics pour déterminer si vous avez déclaré faillite, si vos biens sont assujettis à des droits de nantissement, si vous avez omis de payer des contraventions, si vous êtes impliqué dans une dispute au sujet d'un bien avec un ex-conjoint ou si vous avez déjà été condamné au criminel. L'accès aux données publiques est réglementé par les lois provinciales sur le crédit à la consommation.

Sous-traitance de la surveillance

Nous avons montré à quel point le concept de sous-traitance est devenu banal pour les services publics. Dans le contexte de la surveillance, cette externalisation des fonctions de l'État engendre certains défis et crée de nouvelles zones grises. Comment s'appliquent les exigences de protection des renseignements personnels prévues par la loi lorsqu'il existe deux séries de règles, l'une pour le gouvernement et l'autre pour le secteur commercial ? En 2012-2013, le gouvernement de la Colombie-Britannique et celui de l'Ontario

« Big Brother Inc. » : les groupes de défense des droits protestent contre l'exportation des produits de surveillance

N'oublions pas que si elles sont mises entre les mains de régimes répressifs et autoritaires, ces technologies de surveillance peuvent être létales. Alors, qui vend ces technologies à ces régimes? Que pouvons-nous faire?

Depuis 1995, le groupe militant international, Privacy International, a participé à une campagne d'envergure internationale visant à lever le voile sur les entreprises qui ont vendu les technologies de surveillance aux régimes autoritaires et qui, dans certains cas, l'ont fait en violant les lois internationales et les restrictions de la réglementation des exportations. La campagne, appelée « Big Brother Inc. », visait à dévoiler l'ampleur de la croissance de l'industrie de la surveillance au cours de la dernière décennie et comment ce matériel élimine la liberté d'opinion, fait taire les opinions dissidentes et place les dissidents à la merci de la classe dirigeante lorsqu'il se retrouve dans les mains de régimes répressifs; ce matériel est aussi, sinon plus efficace que les fusils et les bombes[1].

Les régimes répressifs qui respectent peu les libertés civiles s'intéressent particulièrement à l'interception des communications des activistes et des dissidents. Ils se sont donc procuré, auprès d'entreprises principalement occidentales, diverses technologies d'interception des communications et de surveillance des habitudes de navigation. Ils ont notamment fait l'achat de logiciels malveillants qui infectent l'ordinateur ciblé et permettent d'enregistrer chaque mot saisi au clavier, de logiciels de piratage qui enregistrent les communications et les sites consultés sur Internet et même de dispositifs d'interception des données qui transitent par les câbles sous-marins de fibre optique. Privacy International soutient que l'exportation des technologies de surveillance correspond presque à une forme d'exportation d'armes.

De telles pratiques contreviendraient-elles par conséquent à la réglementation générale en matière de contrôle des exportations d'armes? Exigent-elles par conséquent des permis, des certificats de l'utilisateur, etc.? Privacy International a intenté des poursuites dans plusieurs pays. En 2011, le président Obama a signé un décret imposant de nouvelles sanctions et l'interdiction de visas contre les mercenaires du numérique qui créent ou qui exploitent ces systèmes qui sont

ont étudié la possibilité d'utiliser des « identifiants communs » pour les citoyens qui touchent des prestations gouvernementales, comme l'aide sociale ou l'assurance-emploi. Outre la difficulté de gérer les vastes bases de



La dissidence politique est-elle menacée par les technologies de surveillance de l'occident? (Source : © iStockphoto.com/EduardoLuzzatti)

utilisés pour suivre, repérer et cibler les citoyens et pour perpétrer de graves violations des droits de la personne.

Grâce à la recherche et aux enquêtes, aux campagnes de sensibilisation du public, à la mobilisation politique, aux litiges stratégiques, à la dénonciation et à la condamnation, l'organisme est parvenu à obtenir des résultats. Le nom des sociétés et des organismes du gouvernement qui sont impliqués dans ce commerce figure maintenant dans le bottin de la surveillance. Et la liste s'allonge. Les entreprises canadiennes dans tout ça? Cinq d'entre elles figurent dans la liste[2].

1. Privacy International, « Big Brother Inc.: A Global Investigation into the International Trade in Surveillance Technologies », 2012, https://www.privacyinternational.org/projects/big-brother-inc.
2. Privacy International, « Surveillance Who's Who », sans date, http://bigbrotherinc.org/v1/.

données qui sont requises, des problèmes de taille se posent sur le plan de la reddition de comptes : qui sera responsable des données personnelles, les entreprises fournissant l'équipement ou le ministère versant les prestations ?

La gestion de certaines bases de données sera-t-elle confiée à une société privée ? L'identifiant commun finira-t-il par être utilisé pour toutes les transactions du gouvernement avec la personne concernée ? Quels règlements s'appliqueront, ceux s'appliquant au secteur public ou ceux s'appliquant au secteur privé ?

Il devient de plus en plus difficile de répondre à ces questions puisque les partenariats conclus entre les gouvernements et les organismes privés dans la nouvelle industrie de la surveillance sont un phénomène observé à l'échelle mondiale. En effet, dans la plupart des cas, la collaboration est tellement étroite qu'il est impossible de déterminer laquelle des parties est la principale. Dans le cadre de ces collaborations, le secteur public est généralement le bailleur de fonds. Il délègue cependant l'essentiel de la prise de décisions, notamment celles concernant les produits de sécurité à acheter, au secteur privé puisqu'il détient l'expertise reconnue dans le domaine. Or, comme la valeur des contrats gouvernementaux se chiffre en millions de dollars pour les entreprises privées, il est avantageux pour les entreprises spécialisées dans la technologie de créer le plus d'occasions d'affaires possible en vendant de plus en plus de produits de surveillance (sans mentionner les mises à niveau et la maintenance). Elles ont également tout à gagner en renforçant les préoccupations liées à la sécurité qui poussent les gouvernements à faire ces achats.

Le 11 septembre a également eu des répercussions économiques considérables. Bien que les technologies de la surveillance aient déjà joué un rôle important avant les attentats contre le World Trade Center, les débouchés en découlant ont donné un coup d'accélérateur à nombre d'industries du secteur de la sécurité[13]. Les nouveaux systèmes se sont multipliés sous prétexte qu'il faut faire les liens nécessaires et que pour ce faire, on doit avoir recours : au partage de données et à l'exploration de données ; à la surveillance par caméras et aux scanneurs corporels ; à une utilisation accrue des dossiers passagers par les agences des services frontaliers ; au partage international de données ; aux cartes d'identité et aux permis de conduire améliorés ; à l'observation des comportements ; aux technologies biométriques ; et aux drones. Les nouvelles priorités se sont étendues à la « sécurité urbaine » et se situent également dans la ligne des priorités découlant du 11 septembre, notamment les zones d'accès restreint et le renforcement des services de police lors d'événements. Les attentats du 11 septembre ont également accru les façons dont l'information courante, comme celle que l'on retrouve dans les médias sociaux, est affectée à la surveillance aux fins de sécurité[14].

Citons un dernier exemple, celui des gigantesques rassemblements[15]. Parmi ces événements hautement médiatisés, mentionnons les grandes compétitions sportives ou athlétiques, les sommets politiques de haut niveau ainsi que les festivals de musique et les festivals culturels. Ces rassemblements donnent lieu à de vastes opérations de sécurité ; généralement, les entreprises de sécurité se déplacent partout dans le monde pour suivre ces événements. C'est pourquoi de nouveaux liens – et un échange de données – sont créés entre les organismes militaires, gouvernementaux et commerciaux chaque fois qu'un événement de cette envergure est organisé. Les Jeux olympiques d'hiver de Vancouver et le sommet du G20 tenu à Toronto ont engendré des occasions extraordinaires pour le partage de données, d'images vidéo ou de renseignements sur les participants.

Conclusion

En somme, nous ne pouvons que tirer une conclusion plutôt pessimiste : au XXIe siècle, la surveillance au Canada augmente de façon inexorable alors que les données personnelles circulent de plus en plus librement entre les organes publics et privés. Le décloisonnement entre ces secteurs peut être mis en lumière de plusieurs façons, mais les conséquences d'une augmentation de la surveillance sont les mêmes dans chaque cas. Les organismes publics et privés sont investis de mandats différents et sont assujettis à des modes de redditions de comptes distincts ; les données personnelles deviennent donc plus vulnérables aux mauvais usages et aux abus du moment où les flux de données empruntent de nouvelles directions.

Les données recueillies à une certaine fin peuvent facilement être utilisées à une autre fin lorsque les organismes publics et privés échangent des données, ce qui va à l'encontre des pratiques justes de traitement de l'information. Par ailleurs, il devient réellement difficile d'assurer la reddition de comptes pour le traitement des données personnelles lorsque différents régimes juridiques sont censés régir le public et le privé. Du point de vue du citoyen ordinaire, cela signifie que vous ne pouvez jamais vraiment savoir si vos renseignements personnels, qui sont recueillis par le gouvernement ou les services de police, seront communiqués à des entreprises ou si les données glanées des transactions des consommateurs seront évoquées dans un litige sur des prestations gouvernementales ou empêcheront un passager de monter à bord d'un avion. Le réseau complexe et variable de liens

entre les organismes publics et les entreprises du secteur privé, de même qu'entre bien d'autres institutions situées dans la zone grise entre les deux, rend l'analyse complexe, prive les métaphores orwéliennes simplistes de tout sens, pose des difficultés pour les simples citoyens et hypothèque nos lois sur la protection de la vie privée.

Notes

1 Voir Comité de surveillance des activités de renseignement de sécurité, *Review of CSIS's Private Sector Relationships,* SIRC Study 2010-02 (Ottawa, Service canadien du renseignement de sécurité, 14 février 2011).

2 Voir Clinique d'intérêt public et de politique d'Internet du Canada, *On the Data Trail: How Detailed Information About You Gets into the Hands of Organizations with Whom You Have No Relationship—a Report on the Canadian Data Brokerage Industry,* Ottawa, 2006, https://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf/, p. 20 ; et « RCMP Turns to Data Brokers », *Ottawa Citizen*, 30 septembre 2006, http://www.canada.com/ottawacitizen/news/story.html?id=cof14734-9145-4e48-afca-cfec484aea57.

3 Leo Singer, *Accès excessif ?*, *National Actualités et tendances en droit*, Association du Barreau canadien, juin 2012, http://www.nationalmagazine.ca/Articles/June-2012-Issue/Unwarranted-access.aspx.

4 Google, « Transparence des informations », sans date, http://www.google.com/transparencyreport/userdatarequests/.

5 Electronic Frontier Foundation, « NSA Spying on Americans », sans date, https://www.eff.org/nsa-spying.

6 Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz et Amandine Scherrer, *Fighting Cyber Crime and Protecting Privacy in the Cloud*, Étude du Parlement européen, 2012, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf.

7 Ibid., p. 34.

8 « Cloud Computing Law Puts Canadians at Risk of Snooping by US Spies », *Ottawa Citizen*, 2 février 2013.

9 Commissariat à la protection de la vie privée du Canada, *Rapport de vérification sur le Centre d'analyse des opérations et déclarations financières du Canada,* (Ottawa, ministère des Travaux publics et des Services gouvernementaux du Canada, 2009), http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_fintrac_200910_f.pdf.

10 Les plateformes de négociation électronique haute vitesse ont réduit le temps nécessaire pour faire un ordre commercial à 300 microsecondes. Autrement dit, les machines peuvent traiter 100 000 ordres par seconde, donc 500 millions par jour. Dans cette course aux armes technologiques, les prédateurs négociants s'emploient sans relâche à découvrir et à « jouer » les algorithmes des sociétés concurrentes. (La durée utile d'un algorithme est maintenant de 14 jours.) Laureen Snider, « The Technological Advantages of Stock Market Traders », dans Susan Will, Stephen Handelman et David C. Brotherton (dir.), *How They Got Away With It: White-Collar Crime and the Financial Meltdown* (New York, Columbia University Press, 2013), p. 151-170.

11 Canada, Sécurité publique, *Protéger les Canadiens grâce au Programme de protection des passagers*, dernière modification le 12 septembre 2013, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/index-fra.aspx.

12 Colin J. Bennett et Robin M. Bayley, « Les partis politiques fédéraux du Canada et la protection des renseignements personnels : une analyse comparative », rapport commandé par le Commissariat à la protection de la vie privée du Canada, mars 2012, http://www.priv.gc.ca/information/research-recherche/2012/pp_201203_f.asp.

13 Voir, par exemple, Robert O'Harrow, *No Place to Hide* (Toronto, Free Press, 2005).

14 Daniel Trottier, « Policing Social Media », *Canadian Review of Sociology / Revue canadienne de sociologie* 49, nº 4 (2012), p. 411-425.

15 *Security Games: Surveillance and Control at Mega-events*, publié sous la direction de Colin J. Bennett et Kevin D. Haggerty (Londres et New York, Routledge, 2011). Voir aussi http://www.security-games.com.



L'ambiguïté croissante de l'information personnelle

De données identifiées à personnes identifiables

Si le bibliothécaire vous demande une carte d'identité, vous présumez sans doute qu'une carte sur laquelle on retrouve les coordonnées que vous inscrivez habituellement sur une enveloppe suffira. D'autres pourraient vous demander aussi votre permis de conduire, mais qu'en est-il de votre numéro d'immatriculation ou même de votre visage ? S'agit-il de renseignements personnels ? La réponse à cette question n'est pas si évidente et c'est justement là que réside le problème : la signification de renseignements personnels a changé.

Fut un temps où le concept de « renseignements personnels » était relativement clair : il s'agissait de votre nom, votre adresse et peut-être un numéro d'identification officiel utilisé par le gouvernement, comme le numéro d'assurance sociale. De plus, nous savions essentiellement qui utilisait ces renseignements pour nous identifier et quand il le faisait. Il ne fait aucun doute que l'on pouvait parfois se mélanger et faire des erreurs d'identification. Nous étions toutefois identifiés par des moyens que nous connaissions et qui nous paraissaient transparents.

Dans une large mesure, nous nous attendions également à ce que les organismes que nous connaissions protègent notre vie privée et nous comptions sur eux pour le faire. C'est ce qu'ils faisaient en protégeant d'autres renseignements liés à nos identifiants personnels, entre autres, les registres bancaires, les déclarations du recensement, les antécédents de crédits à la consommation et le registre de nos emprunts à la bibliothèque. Enfin,

Votre plaque d'immatriculation est-elle une information personnelle?

En 2011, la Cour d'appel de l'Alberta a conclu que, pour que l'information soit sur une « personne identifiable » au titre du *Alberta Freedom of Information and Protection of Privacy Act*, la personne doit pouvoir être identifiée. Autrement dit, l'information doit avoir un lien précis avec la personne[1]. Cette information doit porter sur la personne, c'est-à-dire qu'elle doit être liée directement à cette personne et ne pas concerner un bien que cette personne pourrait détenir (comme une voiture). Certains renseignements ne sont pas en soi personnels, mais ils le deviennent puisqu'ils sont associés indirectement à une personne par le lien de propriété. Par conséquent, en Alberta, un numéro de permis de conduire est un renseignement personnel, mais un numéro de plaque d'immatriculation ne l'est pas, et ce, même si en Alberta du moins, une plaque d'immatriculation est associée à un véhicule puis peut être liée à une personne au moyen d'une base de données.

Que se passe-t-il donc lorsque les numéros de plaque d'immatriculation sont photographiés automatiquement et identifiés au moyen de caméras qui permettent la reconnaissance automatisée des plaques d'immatriculation? Ces appareils utilisent la reconnaissance optique de caractères pour faire une lecture automatisée des plaques puis faire une recherche dans diverses bases de données. La commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique a fait un constat à la fin 2012 dans ce dossier. Elle a conclu que les gens avaient des attentes à l'égard de la protection des renseignements personnels associés à leur plaque d'immatriculation puisque, bien que le numéro en soi ne permette pas de les identifier, le lien commun entre le numéro et l'information identifiable signifie que l'information devrait être protégée.

Les autorités semblent hésiter entre considérer l'information d'immatriculation comme étant privée ou la considérer comme étant publique. Certains services de police sont d'avis que les photos prises des plaques d'immatriculation ne sont pas un renseignement personnel et peuvent donc être recueillies. Ils soutiennent cependant que le public ne devrait pas avoir accès aux registres créés par ces photos, parce que ceux-ci contiennent des renseignements personnels. La GRC a envoyé une lettre pour reconnaître officiellement que les données amassées au moyen des pratiques des autorités dans ce domaine *sont* des renseignements personnels. Or, le directeur du programme de reconnaissance des plaques de la GRC et d'autres policiers canadiens continuent d'affirmer que comme les plaques d'immatriculation des véhicules sont



Votre plaque d'immatriculation est-elle considérée comme une donnée personnelle? (Source : © iStockphoto.com/tomeng)

visibles en tout temps, le public ne peut raisonnablement s'attendre à ce que ces renseignements soient protégés[2].

Cette confusion vient brouiller la nature politique de la surveillance à grande échelle. Lorsque des données « non personnelles » sont recueillies, il est relativement facile de convaincre le public et les organes de contrôle du gouvernement que la collecte de données est appropriée. Néanmoins, lorsque la surveillance capture des renseignements personnels, des questions de protection juridique et des questions normatives sont soulevées, ce qui peut retarder le déploiement des technologies de surveillance. La question de savoir si les plaques d'immatriculation sont ou ne sont pas une donnée personnelle est devenue fondamentalement un enjeu politique.

1. Alberta, Cour d'appel, *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94 (CanLII), http://canlii.ca/en/ab/abca/doc/2011/2011abca94/2011abca94.html.
2. Christopher A. Parsons, Joseph Savirimuthu, Rob Wipond et Kevin McArthur, « ANPR: Code and Rhetorics of Compliance », Social Science Research Network, 4 septembre 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2141127, p. 12.

si nous ne voulions pas qu'un inconnu nous contacte, nous n'avions qu'à demander un numéro non inscrit.

Les temps changent.

Récemment, le ministre de la Sécurité publique du Canada a défendu les tentatives visant à actualiser et à accroître la capacité des organismes d'application de la loi d'avoir accès à l'information qui permet de nous identifier lorsque nous naviguons sur Internet. Il a alors déclaré que les divers moyens pour nous identifier sur le Web ne sont pas différents des annuaires téléphoniques dans lesquels figurent notre numéro de téléphone, notre nom et notre adresse résidentielle. Comme les policiers peuvent trouver l'abonné auquel est associé un numéro de téléphone, ils devraient également pouvoir savoir qui se trouve derrière les multiples identifiants qui permettent à chacun d'entre nous de communiquer et de réseauter sur le Web. Dans le cas présent, le gouvernement fait une différence qui l'arrange bien, mais qui est douteuse, entre les « données des abonnés », pour lesquelles les policiers n'ont pas besoin de mandat – comme ils n'ont pas besoin de mandat pour chercher une personne dans l'annuaire téléphonique – et le contenu des communications, qui lui requiert une demande préalable d'autorisation judiciaire (un mandat) reposant sur des motifs raisonnables et probables de croire qu'un crime a été commis ou sera commis.

Les renseignements sur les abonnés diffèrent toutefois de l'inscription dans l'annuaire[1]. La façon dont nous sommes identifiés sur le Web est complexe et dynamique. Nos communications électroniques font intervenir beaucoup d'autres identifiants que notre nom, notre numéro de téléphone et notre adresse. Combien d'entre nous connaissent ou peuvent décoder les concepts suivants : l'adresse IP (Internet Protocol), le numéro d'identification mobile, l'adresse MAC (Media Access Control), le code identificateur du fournisseur de service, le numéro de série électronique, l'identité internationale d'équipement mobile, l'identité internationale de l'abonné mobile, et le module d'identification de l'abonné (la fameuse carte SIM) ? Chacun de ces identifiants peut servir à isoler un utilisateur. Voilà donc le premier élément de cette tendance : nous sommes maintenant identifiés par des moyens hi-tech qui restent mystérieux pour le commun des mortels. La plupart d'entre nous n'ont aucune idée de la façon dont nous sommes identifiés en ligne.

Le second facteur est que nous n'utilisons pas Internet de la même façon que nous utilisons un téléphone. L'Internet n'est pas seulement un moyen de communication. Ce réseau est la plateforme de base dont beaucoup d'entre nous se servent pour accomplir des tâches professionnelles,

personnelles et politiques indispensables. Nous l'utilisons pour réserver des chambres d'hôtel et des vols, pour contacter nos amis et nos collègues par les médias sociaux, pour acheter des livres et de la musique, pour organiser nos vies au moyen de calendriers et pour faire des recherches. Ces renseignements peuvent en dire beaucoup plus sur notre vie que ce qui peut se dire lors d'une conversation téléphonique. Ainsi, la façon dont nous sommes identifiés dans les réseaux numériques fournit des indications importantes qui permettent de déterminer qui nous sommes, ce que nous faisons, avec qui nous le faisons et où et quand nous le faisons.

Par conséquent, lorsqu'ils passent au peigne fin les identifiants, les organismes peuvent obtenir une grande quantité de données sur notre vie quotidienne. Vous pouvez vérifier qui pourrait avoir accès aux données sur vos habitudes de navigation en installant une application gratuite comme Collusion ou Ghostery. En quelques secondes, vous verrez apparaître une liste des réseaux de publicités ou des outils d'analyse ou de rapport cybermétrique qui enregistrent et partagent vos activités sur le Web. Si vous continuez de naviguer sur Internet, la liste s'allongera et ses ramifications s'étendront comme une toile d'araignée. Dans le monde virtuel, nous sommes maintenant « identifiables », même si nous ne sommes pas « identifiés ».

Les adresses IP et MAC sont-elles des renseignements personnels ?

Un numéro unique, appelé adresse IP (Internet Protocol), est attribué à chaque appareil connecté au réseau Internet public. Ce numéro permet aux applications d'envoyer les informations, comme des résultats de navigation ou des courriels, au bon destinataire. L'adresse IP est composée de quatre groupes de chiffres séparés par des points. Comme ces nombres sont généralement assignés aux fournisseurs d'accès Internet par bloc de régions, l'adresse IP peut souvent être utilisée pour localiser un utilisateur. Cette question est toutefois beaucoup plus complexe, car certaines adresses IP sont dynamiques et changent fréquemment.

Le Commissariat à la protection de la vie privée du Canada considère que l'adresse IP est un renseignement personnel :

> L'adresse de protocole Internet (IP) peut être considérée comme un renseignement personnel si elle peut être associée à un individu identifiable. Par exemple, dans une conclusion d'enquête, nous

> avons déterminé que quelques-unes des adresses IP recueillies par un fournisseur de services Internet (FSI) étaient des renseignements personnels, car le FSI pouvait associer ces dernières à ses clients au moyen du numéro d'abonné[2].

En dépit de ces décisions, un débat important a cours depuis longtemps sur la question : l'adresse IP est-elle considérée ou n'est-elle pas considérée comme un renseignement personnel au titre des dispositions législatives sur la protection de la vie privée. La réponse à cette question est cruciale pour déterminer si l'utilisateur moyen d'Internet a droit à la protection de sa vie privée lorsqu'il fait des recherches, navigue sur le Web, écrit un billet sur son blogue ou utilise les médias sociaux. Selon la position officielle de Google, l'adresse IP ne constitue pas un renseignement personnel puisqu'elle permet d'identifier une machine et non une personne[3]. Plusieurs utilisateurs peuvent se partager un seul ordinateur, lequel a une seule adresse IP. Citons par exemple les membres d'une même famille, les employés d'une entreprise ou des étudiants qui se partagent les ordinateurs de la bibliothèque. Un fournisseur d'accès Internet peut donc associer l'adresse IP à une maison ou à une entreprise, mais il ne pourrait pas l'associer à la personne qui a utilisé l'appareil connecté à Internet, du moins il ne peut habituellement pas le faire.

Par ailleurs, en raison de la mobilité de nos appareils, nous nous connectons souvent à Internet dans des cafés, à l'aéroport et dans d'autres endroits publics et nous le faisons en utilisant de multiples adresses IP. De plus, l'utilisation croissante de la commande d'accès au support (MAC) exacerbe les préoccupations au sujet de la protection de la vie privée. L'adresse MAC est un numéro qui permet d'identifier de manière unique les appareils mobiles, tels que les cellulaires, les iPods, les ordinateurs portables ou les tablettes, sur un réseau.

Or, ce n'est pas parce que les appareils et les adresses ne sont pas fixes que les protocoles d'adressage n'entrent pas dans la catégorie de renseignements personnels. Même si je change mon numéro de téléphone résidentiel chaque semaine, celui-ci demeurera un renseignement personnel. Peut-on réellement conclure qu'il n'existe aucun risque d'atteinte à la vie privée simplement parce qu'on ne peut pas attribuer une trace à une personne ? Pour répondre, il faut savoir qu'à partir d'un petit groupe de personnes actives sur le Web, un tiers peut départager, puis associer son comportement individuel à chaque membre du groupe.

Bien qu'une adresse MAC ou IP permette rarement d'identifier directement une personne, c'est la combinaison – ou la combinaison qui pourrait raisonnablement être faite – de ces adresses avec d'autres renseignements sur les goûts, les habitudes et les intérêts qui inquiète les défenseurs de la vie privée[4]. Ainsi, si l'on connaît suffisamment d'informations en ligne et hors ligne et que l'on combine ces renseignements, on pourrait disposer de suffisamment de données pour avancer une supposition hautement vraisemblable (parfois, presque parfaite) sur qui faisait quoi, quand et où.

Identification et réidentification

Dans le même ordre d'idées, il est possible d'identifier une personne, même si l'on ne dispose pas de renseignements nominatifs comme son nom ou son adresse. Selon une étude récente menée auprès d'un échantillon aléatoire de personnes habitant à Montréal, près de 98 % des gens peuvent être identifiés par leur nom si l'on connaît les trois variables suivantes : date de naissance, sexe et code postal[5]. Les chercheurs ont indiqué que ces conclusions avaient des conséquences particulièrement préoccupantes dans le cadre de la recherche en santé puisque les gens hésitent moins à divulguer des données sur leur santé, si le risque de réidentification est faible.

La science de la réidentification sert à identifier une personne unique, en dépit des efforts déployés pour retirer les identifiants évidents des ensembles existants de données (processus appelé dénominalisation ou anonymisation). La puissance de certaines techniques de réidentification a fait dire à certains chercheurs que la dénominalisation donne une fausse impression que l'anonymat est préservé. En fait les pratiques courantes de préservation de l'anonymat ne permettent plus de protéger la vie privée, parce que la science de la réidentification a bouleversé les hypothèses élémentaires au sujet de ce qui est et de ce qui n'est pas une donnée personnelle. Elle a aussi obligé les organes de réglementation et les analystes à revoir les principes fondamentaux de la protection de l'information. La vérification de l'identité ne repose plus sur un choix entre les données identifiantes et celles qui ne le sont pas. Elle repose plutôt sur un continuum complexe et dynamique qui dépend des autres renseignements qui pourraient plus tard être liés à ceux déjà recueillis. Bref, les risques pour les particuliers ne se dissipent pas lorsque les identifiants personnels sont enlevés. Et il ne s'agit pas seulement d'une question scientifique et théorique : des intérêts économiques

Une image faciale est-elle une information personnelle?

Ayan marche dans la rue Sherbrooke à Montréal; ses amis et les gens qui la connaissent reconnaissent son visage. Si ces gens la connaissent suffisamment, ils peuvent associer son visage à son nom. Cette situation a poussé certains à croire qu'Ayan, comme toutes les autres personnes dans un endroit public, ne peut s'attendre raisonnablement à ce que sa vie privée soit protégée. Comme Ayan a choisi de se présenter en « public », elle abandonne du même coup son droit à la vie privée.

Toutefois, les choses ne sont pas aussi simples qu'elles en ont l'air. Si la boutique de vêtements où Ayan entre capture une image d'elle sur ses caméras de surveillance, cela signifie-t-il qu'Ayan a renoncé à son droit de contrôler de quelle façon cette image sera utilisée et qui pourrait y avoir accès? Nos lois indiquent que non. Même si cette image ne peut être associée immédiatement à Ayan, comme une « personne identifiable », les organisations sont tenues par la loi de protéger ces données et de les utiliser uniquement à des fins légitimes. Par ailleurs, comme Ayan et beaucoup d'autres utilisent les médias sociaux, la situation se complique davantage. Les médias sociaux utilisent un logiciel d'imagerie physionomique qui permet à Ayan et à ses amis d'étiqueter les images au moyen d'identifiant et de les diffuser largement.

Ces logiciels sont assortis d'algorithmes qui mesurent les traits faciaux (positionnement relatif des yeux, du nez, des pommettes et de la mâchoire, leur taille et leur forme). Les mesures ainsi obtenues peuvent ensuite servir à chercher d'autres images correspondant aux mêmes données dans d'autres bases de données. L'étiquetage des photos sur les médias sociaux, comme Facebook, suscite la controverse et a incité les défenseurs du droit à la vie privée à protester. À la fin 2012, Facebook s'est engagé à renoncer à son programme d'étiquetage des visages après que les organes de réglementation et les défenseurs de la vie privée eurent manifesté leur désaccord. Cependant, cette pratique se poursuit encore.

Les conséquences sur la vie privée découlant de l'association pouvant être faite entre le visage d'Ayan et son nom sont colossales. Outre l'usage que pourraient en faire les organismes d'application de la loi, ces technologies ont été décrites comme « l'outil rêvé des traqueurs ». Oui, le visage d'Ayan et le vôtre constituent un renseignement personnel. Et, oui, nous devrions pouvoir exercer des droits quant à la façon dont cette information est capturée et diffusée.



Reconnaissance faciale : qui devrait avoir accès aux données de votre image faciale? (Source : © iStock-photo.com/rappensuncle)

colossaux sont en jeu. L'augmentation de l'utilisation d'Internet et la prolifération des technologies de communication font s'accroître l'accessibilité à l'information, ce qui alimente l'autonomisation individuelle et la participation démocratique. Parallèlement, grâce à l'Internet, il est beaucoup plus facile pour les organismes d'enregistrer de l'information au sujet des particuliers, de la traiter et de la diffuser, et ce, souvent par des moyens cachés. Un vaste éventail d'entités peut maintenant observer les comportements en ligne en surveillant le réseau, en puisant dans la mine de données recueillies au sujet de l'utilisation d'Internet par les particuliers ou en installant un logiciel espion directement sur des ordinateurs personnels. Les annonceurs tiers n'ont pas besoin de connaître votre « identité » réelle pourvu qu'ils puissent vous identifier avec une adresse technique puis vous cibler avec des publicités personnalisées.

Le traitement de renseignements de nature personnelle est par conséquent un élément fondamental des modèles d'affaires grâce auxquels les entreprises de données de masse génèrent des profits. La publicité est le nerf de la guerre dans l'économie de l'Internet. Dans la mesure où les entreprises découvriront de l'information plus détaillée et plus complète au sujet des préférences personnelles et des comportements, elles augmenteront leurs revenus. Néanmoins, les lois sur la protection des renseignements personnels limitent en quelque sorte cette capacité. Les règlements touchant notamment les avis, le consentement éclairé, l'accès et la correction de données personnelles ne sont pas seulement un obstacle important à la capacité d'un organisme de surveiller les consommateurs ; ils ont également des conséquences économiques profondes. Il en va de même pour la définition de renseignements personnels et du débat entourant ce qui est considéré et ce qui n'est pas considéré comme un renseignement personnel. Si le renseignement est « personnel », les organismes ont des contraintes. S'il ne l'est pas, ils ne sont pas réglementés.

Contenu généré par l'utilisateur

Le réseautage social constitue une autre source de confusion au sujet de la notion traditionnelle de « renseignements personnels ». À l'ordinaire, nous pensons que les questions de vie privée découlent de la collecte et du traitement par les organismes de renseignements personnels au sujet de particulier. Essentiellement, ce sont les grands organismes qui gèrent les

données personnelles ; ils les analysent au moyen de technologies de pointe afin de prendre des décisions relatives aux particuliers à titre, entre autres, de consommateurs, de clients, d'étudiants et d'employés.

Or, dans l'univers des réseaux sociaux, ce sont les particuliers qui génèrent le plus de données. On entend par « contenu généré par l'utilisateur » (CGU), ou « contenu généré par les consommateurs » le contenu créé et partagé sur le Web par les usagers ; ce contenu va d'un commentaire sur un livre laissé sur le site Amazon.com à la vidéo partagée sur YouTube en passant par les profils Facebook. Le contenu généré par l'utilisateur est un concept qui est présent sous diverses formes depuis les balbutiements d'Internet. Cependant, dans les dernières années, il est devenu l'une des formes de contenu affichant la croissance la plus rapide en raison de l'accès de plus en plus grand à Internet haute vitesse et des technologies de recherche. De plus, il a révolutionné la façon dont les usagers interagissent entre eux et dont les annonceurs touchent ces individus.

Dans le contenu généré par les utilisateurs, les renseignements personnels appartiennent-ils à l'utilisateur ou à l'entreprise à qui appartient la plateforme hôte ? Ces entreprises sont-elles tenues d'appliquer tous les principes de protection de la vie privée aux données que nous fournissons ? Nos organes de réglementation ont tendance à répondre oui à cette question ; ils insistent sur le fait que les services de réseautage social agissent comme contrôleurs de données, peu importe d'où proviennent les données personnelles traitées[6].

Cependant, les entreprises tendent à voir les choses différemment et cette vision ressort dans les définitions de « renseignements personnels » que l'on trouve dans leurs politiques officielles sur la protection des renseignements personnels. D'ailleurs, une étude récemment réalisée sur les 24 sites de réseautage social les plus utilisés au Canada le prouve[7]. Comme on peut s'y attendre, la notion de ce qui caractérise de façon précise une information permettant d'identifier une personne varie sur tous ces sites. En voici quelques exemples :

- *Google* (Blogger et Google+) : Information que l'utilisateur fournit à Google et qui permet de l'identifier, comme le nom, l'adresse courriel, les renseignements sur la facturation ou d'autres données que Google pourrait lier à juste titre à ces renseignements.
- *Facebook* : Le nom, les photos de profil et même les photos de couverture, le réseau, le sexe, le nom d'utilisateur et

l'identification de l'utilisateur. Facebook peut consigner l'adresse IP, l'emplacement géographique, le fournisseur d'accès Internet, l'emplacement, le type de navigateur ou les pages que vous visitez.

- *Flickr* : Le nom, le sexe, la date de naissance, le code postal et l'adresse courriel. Flickr recueille des renseignements au sujet des opérations des usagers avec Yahoo et avec ses partenaires commerciaux, dont de l'information sur l'utilisation par les usagers des produits et des services financiers qu'ils offrent.
- *Instagram* : La quantité et le type d'information qu'Instagram recueille dépendent de la nature de l'interaction.
- *Plenty of Fish (POF)* (un site de rencontre canadien) : coordonnées, préférences personnelles (langues choisies), renseignements à caractère commercial (photographies), autres renseignements fournis sur le profil de la personne (intérêts, état civil, taille, poids, profession).
- *Zynga* : Nom, photo de profil ou l'adresse URL qui y est associée, numéro d'identification de l'utilisateur, numéro d'identification des amis de l'utilisateur et autres données publiques, courriel utilisé pour la connexion, emplacement physique et celui des appareils, sexe, date de naissance.

Toutes ces définitions ont des conséquences sur la protection de la vie privée. À titre d'exemple, Nexopia s'annonce sur son site comme le premier site de réseautage social pour les jeunes en importance au Canada. Il conseille également aux utilisateurs de soumettre et d'afficher des données supplémentaires sur leur profil pour aider les autres utilisateurs à les trouver et à communiquer avec eux. Il suggère notamment de dévoiler son poids, sa taille, son orientation sexuelle, sa situation amoureuse et son cadre de vie, et ses intérêts[8]. Il est entendu que ces renseignements ne sont pas obligatoires pour utiliser Nexopia ; cependant, comme ce ne sont pas tous les renseignements fournis dans le profil d'un utilisateur qui entrent dans la catégorie « données personnelles recueillies », ces renseignements pourraient être partagés.

Il semble que Ping, l'application de réseautage social d'Apple pour la musique, fournisse une catégorie d'information personnelle protégée à ses utilisateurs. L'application restreint toutefois cette catégorie aux coordonnées et aux renseignements sur les paiements. Cette catégorie n'inclut pas l'information recueillie au sujet de la famille et des amis de l'utilisateur ; lorsque

l'utilisateur partage ses chansons préférées avec les autres, « Apple peut collecter les renseignements que vous fournissez sur ces personnes, notamment leur nom, leur adresse postale, leur adresse électronique et leur numéro de téléphone »[9]. En clair, Apple recueille de l'information personnelle de tiers et, comme la politique de confidentialité de l'entreprise ne s'applique pas à ces tiers, Apple ne considère pas ces données comme des renseignements personnels.

N'oublions pas la question des métadonnées, soit les données qui renseignent sur des données. Elles comprennent généralement les identifiants, comme l'adresse IP et le système d'exploitation de l'utilisateur, de même que l'information tirée des fichiers de témoins. Ces métadonnées peuvent ensuite être utilisées non seulement pour identifier des personnes et leurs habitudes de navigation, mais également pour déterminer leur emplacement géographique. Des 24 sites de réseautage social visés par le projet de recherche, aucun n'a indiqué que les métadonnées font partie des renseignements personnels et aucun ne crée d'attentes sur le plan de la protection des métadonnées aux utilisateurs. Il n'est donc pas étonnant que les sites de réseautage social justifient le traitement des métadonnées comme une nécessité pour améliorer l'expérience de l'utilisateur. Les adresses IP ou l'information des fichiers témoins (*cookies*) sont nécessaires, affirme-t-on, pour regrouper les services, prévenir les problèmes, sécuriser les produits et adapter en général l'utilisation pour une approche plus « personnalisée ». Les répercussions globales sur la vie privée sont rarement abordées.

Nombre de réseaux sociaux – en fait, nombre de sites Web – permettent aux utilisateurs d'y accéder au moyen de pseudonymes qui dissimulent l'identité de l'utilisateur ; ces mêmes sites permettent toutefois aux utilisateurs de se faire reconnaître automatiquement lors de leur prochaine visite sur la page. On appelle parfois ces pseudonymes des identifiants uniques et on les conçoit intentionnellement de manière à ce qu'ils soient indécodables, bien qu'on puisse manifestement les relier à une personne en particulier. Les gens s'en remettent à cette forme d'identification pour différents scénarios et contextes sur Internet puisque ces pseudonymes font appel à leur candeur et à leur ouverture. Les gens ont toutefois tendance à opter pour le même pseudonyme sur différents sites Web, ce qui facilite leur réidentification.

Comme les entreprises en ligne tirent des profits de ces données, ne devrions-nous pas avoir des droits quant à leur utilisation ? Dans ce cas, comment ferions-nous pour exercer ces droits si l'une des conditions d'utilisation du service requiert l'authentification de notre identité ? On crée donc

un cercle vicieux : une personne doit révéler son identité pour exercer ses droits quant aux données personnelles, qui étaient protégées à la base.

Que dit la loi canadienne au sujet de l'information permettant d'identifier une personne ?

Au cours des trente dernières années, les gouvernements fédéral et provinciaux au Canada ont adopté progressivement des dispositions législatives sur la protection des renseignements personnels. Au départ, la plupart de ces lois réglementaient le secteur public et ce n'est que plus tard qu'elles s'étendirent au secteur privé. Sauf quelques exceptions, la majorité des organismes au Canada – publics et privés – doivent appliquer une série commune de principes de protection de l'information. Or, comme on peut s'y attendre, la définition des éléments qui constituent des renseignements personnels prévue dans les lois n'est pas homogène.

Dans la plupart des lois, on tend à utiliser l'expression « information identifiable ». Ainsi, la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* stipule que les « renseignements personnels [sont] tout renseignement concernant un individu identifiable »[10]. Cette définition est très élastique, mais elle peut également être plutôt circulaire.

Par ailleurs, d'autres lois définissent de façon précise les types particuliers de données personnelles ; elles comprennent notamment de longues listes de catégories de données auxquelles les lois s'appliquent. À titre d'exemple, voici la liste figurant dans la *Loi sur l'accès à l'information et la protection de la vie privée* de l'Ontario :

> (a) des renseignements concernant la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial de celui-ci ;
> (b) des renseignements concernant l'éducation, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de ce particulier ou des renseignements reliés à sa participation à une opération financière ;
> (c) d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué ;
> (d) de l'adresse, du numéro de téléphone, des empreintes digitales ou du groupe sanguin de ce particulier ;

(e) de ses opinions ou de ses points de vue personnels, sauf s'ils se rapportent à un autre particulier ;
(f) de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel, adressée par le particulier à une institution, ainsi que des réponses à cette correspondance originale susceptibles d'en révéler le contenu ;
(g) des opinions et des points de vue d'une autre personne au sujet de ce particulier ;
(h) du nom du particulier, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres renseignements personnels au sujet du particulier[11].

Dans d'autres lois canadiennes, les catégories d'information de nature délicate et non délicate sont légèrement différentes. Reste que ces listes ne peuvent jamais être exhaustives et que la définition de ce qui est un renseignement de nature délicate et de ce qui ne l'est pas est invariablement subjective et en soi liée au contexte. À titre d'exemple, il peut être à notre avantage de faire inscrire notre nom et notre adresse dans l'annuaire téléphonique. Cependant, si la même information figure sur une liste noire, une liste des personnes interdites de vol ou un dossier de mauvais risque de crédit, elle devient hautement délicate. Autrement dit, une même information selon le contexte dans lequel elle est utilisée et selon la fin pour laquelle elle est employée peut avoir une incidence radicale sur le risque d'atteinte à la vie privée.

À l'instar de la loi en Ontario, nombre d'autres lois stipulent que les renseignements doivent être « consignés ». Qu'entend-on par « consigner » ? Une personne a-t-elle des droits sur ses données personnelles même si ces données ne sont pas consignées ? La loi visant le secteur privé au Québec est quelque peu différente ; elle stipule que : « est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »[12].

Dans d'autres lois, on trouve une liste des renseignements qui n'y sont pas assujettis : les coordonnées d'affaires de base ou, de façon plus controversée, l'information sur un produit de travail produite par les travailleurs dans le cadre de leur emploi, dans l'exploitation de leur entreprise ou dans l'exercice de leur profession. L'élargissement de cette exemption, pour inclure les ordonnances médicales signées par des médecins canadiens, est venu alimenter la polémique. De plus, l'exemption portant sur le produit du travail

a également tendance à exclure les données présentées au sujet d'une entreprise sur des sites Web de renseignements sur la consommation comme www.travelocity.com ou www.yelp.com. Il ne serait aucunement raisonnable de demander aux entreprises de consentir avant qu'un consommateur partage une évaluation de son expérience dans un hôtel ou un restaurant. Mais, qu'en est-il des évaluations des professeurs sur le site www.ratemyprofessor.ca ? Les renseignements personnels appartiennent-ils au professeur ou à l'étudiant, ou aux deux ?

Le Commissariat à la protection de la vie privée du Canada a souvent peine à déterminer si oui ou non de l'information personnelle, telle qu'elle est définie dans les lois fédérales s'appliquant au secteur public et au secteur privé (respectivement, la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*), est traitée et, par conséquent, si les dispositions législatives s'appliquent. Dans nombre de cas, le risque d'atteinte à la vie privée repose souvent sur des questions épineuses de probabilité. Nos commissaires et les tribunaux s'évertuent à appliquer un cadre juridique qui est en constante évolution et qui semble toujours être un peu en retard par rapport à la technologie.

Conclusion

La définition contestée et nébuleuse de « renseignement personnel » met en lumière un problème fondamental, soit le fait d'essayer d'utiliser les lois sur la protection de la vie privée pour résoudre le vaste éventail de problèmes sociaux sous-jacents au mot « surveillance » : *la surveillance peut être effectuée même si des renseignements personnels ne sont pas recueillis*. Les exemples cités précédemment montrent que les renseignements personnels qui sont accessibles en ligne ne peuvent être divisés en deux catégories distinctes ; certains renseignements sont personnels tandis que d'autres ne le sont pas. Les risques d'atteinte à la vie privée dépendraient plutôt des hypothèses qu'émettent les organismes à notre sujet lorsqu'ils recueillent de l'information personnelle et de la probabilité qu'ils soient en mesure d'utiliser notre information pour nous identifier. L'analyse des risques pourrait bien être fondée sur des jugements subjectifs au sujet des motivations organisationnelles. D'ailleurs, ce n'est pas parce qu'un organisme peut identifier une personne qu'il le fera.

Dans cette tendance, nous faisons également face à une question plus vaste : comment devons-nous comprendre ce problème social imminent sur le plan politique ? La portée des analyses des facteurs relatifs à la vie privée et des lois sur la protection de la vie privée a tendance à se limiter aux renseignements personnels ou à l'information identifiable. Si on ne peut affirmer qu'il y a un lien réel ou possible entre une pratique de surveillance et une personne en particulier, le cadre de la protection des renseignements personnels ne s'applique pas.

Cependant, l'un des principaux apports des travaux de recherche sur la surveillance est qu'il existe un rapport de pouvoir entre le surveillant et le surveillé, et ce, même si *aucun* renseignement personnel n'est recueilli. D'ailleurs, les caméras de surveillance n'ont pas besoin de fonctionner ou d'être surveillées pour influencer les comportements. La possibilité qu'une surveillance soit effectuée suffit souvent. Même si une personne n'est pas surveillée en tout temps, elle ferait bien de se comporter comme si elle l'était. La même logique accable la collecte d'information au moyen de dispositifs omniprésents comme les appareils informatiques, les capteurs à distance, les drones ou les étiquettes d'identification par radiofréquence ; ces étiquettes permettent un transfert sans fil de données au moyen des ondes électromagnétiques et sont utilisées par de nombreuses industries pour suivre l'emplacement des produits. De plus, même si nos habitudes de navigation sur Internet ne sont pas surveillées, beaucoup d'entre nous en savent suffisamment sur les possibilités de surveillance pour faire attention et prendre des mesures de protection ou peut-être ne pas faire de recherche sur certains sujets.

Les technologies de surveillance structurent les rapports de pouvoir et créent un déséquilibre entre les personnes, de même qu'entre les personnes et les organismes, et ce, même si aucune donnée personnelle n'est amassée. Pourtant, sans données personnelles il est souvent difficile de concevoir qu'un problème de vie privée existe. Or, le pouvoir est exercé ou peut être exercé sans que des données personnelles soient recueillies ou que l'anonymat soit levé. La complexité et l'ambiguïté grandissantes de ces questions mettent en évidence l'éventail de problèmes liés à la surveillance qui ne sont pas inscrits dans la très grande sphère de la protection de la vie privée[13].

Note

1 Canada, Commissariat à la protection de la vie privée, *Ce qu'une adresse IP peut révéler à votre sujet ; Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada,* mai 2013, http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_f.asp.

2 Canada, Commissariat à la protection de la vie privée, *Renseignements juridiques associés à la LPRPDE*, dernière modification le 2 octobre 2013, http://www.priv.gc.ca/leg_c/interpretations_02_f.asp.

3 Alma Whitten, « Are IP Addresses Personal ? », Google Public Policy Blog, 22 février 2008, http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html.

4 Paul Ohm, « Broken Promises of Privacy: Responding to the Surprising Failures of Anonymization », *UCLA Law Review* 57 (2010), p. 1701-1777.

5 Khaled El Emam, David Buckeridge, Robyn Tamblyn, Angelica Neisa, Elizabeth Jonker et Aman Verma, « The Re-identification Risk of Canadians from Longitudinal Demographics », *BMC Medical Infomatics and Decision Making*, 11, nº 46 (2011), http://www.biomedcentral.com/1472-6947/11/46.

6 Voir, par exemple, Groupe de travail «Article 29», *Opinion 5/2009 on Online Social Networking,* Union européenne, adopté le 12 juin 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

7 Colin J. Bennett, Adam Molnar, Christopher Parsons, Brittany Shamess et Michael Smith, *An Analysis of SNS Policies,* rapport non publié financé par l'intermédiaire du Programme des contributions de Commissariat à la protection de la vie privée du Canada, 2012.

8 Voir Nexopia, *Politique de confidentialité*, dernière modification le 31 mai 2013, www.nexopia.com/privacy.

9 Voir Apple Inc., *Politique de confidentialité*, dernière modification le 21 mai 2012, http://www.apple.com/ca/fr/privacy/.

10 Canada, Ministère de la Justice, *Loi sur la protection des renseignements personnels et les documents électroniques*, paragraphe 2(1), http://laws-lois.justice.gc.ca/fra/lois/P-8.6/page-1.html#h-3.

11 Ontario, *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, chapitre F.31, paragraphe 2(1).

12 Québec, *Loi sur la protection des renseignements personnels dans le secteur privé*, chapitre P-39.1, article 2, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1.html.

13 Voir Colin J. Bennett, « In Defense of Privacy: The Concept and the Regime », *Surveillance and Society* 8, nº 4 (2011), p. 485-496.



Augmentation de la surveillance mobile et de la géolocalisation

De qui êtes-vous à où êtes-vous ?

Il y a moins de cinq ans, bon nombre d'experts d'Internet affirmaient encore que les nouvelles technologies de l'information et de la communication (TIC) rendraient la géographie insignifiante. Ce pronostic était fondé sur la conviction que la technologie nous permettrait de communiquer sans encombre avec des gens partout dans le monde, d'obtenir l'information et le contenu que nous souhaitions à partir de n'importe où, ou de travailler aussi bien dans un bureau qu'à la maison ou dans un café à Antigua. Bien que nombre de ces prévisions se soient concrétisées, les capacités de surveillance prises en charge par les technologies qui rendent ce type d'avancées possible ont, au contraire, renforcé l'aspect géographique. Cela, justement parce que notre position est incertaine. Ce besoin, et cette capacité accrue de suivre et de repérer des personnes, constituent une autre grande tendance de la surveillance au Canada et dans d'autres pays.

Prenons par exemple l'évolution de l'utilisation du téléphone avec les années. Il n'y a pas si longtemps, peu de personnes auraient commencé une conversation téléphonique par la question : « Où es-tu ? » Un numéro de téléphone désignait un endroit ; il était l'équivalent d'une adresse municipale. Aujourd'hui, avec l'omniprésence des téléphones portables, votre interlocuteur peut se trouver pratiquement n'importe où sur la planète. Parallèlement, la technologie dépend de données approximatives sur l'emplacement pour pouvoir acheminer les appels au téléphone du destinataire, peu importe où il se trouve.

De plus, nous pouvons maintenant localiser plus efficacement un téléphone. Les premiers réseaux cellulaires pouvaient localiser un téléphone dans un rayon de cent mètres. Lorsque le système de localisation GPS est devenu accessible au public en 2000*, les utilisateurs ordinaires recevaient des données fines sur la position. De nos jours, les téléphones portables ont la capacité d'établir leur position géographique à 2 m près[1]. Le nombre d'appareils prenant en charge les données GPS a champignonné puisque le coût unitaire des puces GPS s'est abaissé au point où on a pu en ajouter à tous les appareils sans que cela ne fasse augmenter considérablement le coût de fabrication. La plupart des nouvelles puces sont compatibles avec d'autres systèmes de navigation par satellite, comme le système russe GLONASS, le Compass en Chine et le futur Galieo de l'Union européenne, via l'Agence spatiale européenne. La multiplication des systèmes et l'essor du marché, où les infrastructures de géolocalisation et de navigation par un système de satellites se livrent concurrence, devrait permettre de produire des données de localisation, plus précises, et ce, plus rapidement et à un plus faible coût**.

Autrefois, on associait possession d'un téléphone portable (ou « cellulaire », comme on disait à l'époque) à richesse et utilisation d'une ligne terrestre à pauvreté. Or, les appareils qui prennent en charge les données GPS sont devenus si abordables aujourd'hui que ce clivage s'est estompé. Même les téléphones cellulaires « gratuits » les plus rudimentaires sont assortis de la capacité de nous localiser. En fait, comme les appareils mobiles deviennent de plus en plus puissants, nombre de consommateurs à faible revenu ont tendance à les utiliser en remplacement de leur ordinateur personnel[2].

Cette capacité de localisation sera bientôt disponible pour des objets de tous les jours au moyen des puces d'identification par radiofréquence, qui rendront ces objets identifiables, ainsi qu'au moyen des plus récents systèmes de protocole Internet qui permettent en théorie qu'une adresse IP soit assignée à presque chaque objet sur la terre. Des capteurs qui peuvent lire les étiquettes puis communiquer l'information sur leur emplacement par réseau

* Il n'est plus convenable d'appeler ces systèmes GPS, puisque ces trois lettres désignent spécifiquement le système étatsunien, qui n'est qu'un parmi d'autres. Il faudrait plutôt parler de géolocalisation et navigation par un système de satellites ou GNSS. Or, comme il s'agit d'un terme répandu, nous emploierons GPS dans cet ouvrage.

** Bon nombre d'observateurs ont soulevé des questions au sujet des répercussions de ces données sur les populations vulnérables, comme les femmes qui tentent d'échapper à une relation violente.

pulluleront dans nos maisons et nos bureaux, dans les immeubles publics et le long des rues, ce qui permettra d'établir la cartographie en temps réel de ces objets (y compris des humains). Il s'agit du concept « d'Internet des objets » dont on a fait étalage ; dans ce réseau, le monde physique et les flux d'information deviendront des strates de notre vie quotidienne. Dans le futur, le simple fait de marcher dans la rue générera un flux d'information contenant les moindres détails de nos interactions courantes avec notre environnement.

Ces percées foisonneront au cours des prochaines années, car il semble qu'elles présentent des avantages tant pour les personnes qui font le suivi que pour celles qui sont suivies. D'ailleurs, elles représentent une forme de surveillance qui revêt une importance particulière et qui croît rapidement. Dans les pages suivantes, nous nous pencherons sur quelques aspects déterminants du potentiel de repérage géographique de masse des objets et des personnes. Nous nous concentrerons sur le repérage à grande échelle dans la vie de tous les jours ; nous n'aborderons pas la question du repérage fait par les policiers ou les services de renseignements ou d'autres formes de localisation auxquelles ont recours les organes d'application de la loi.

Comparaison entre géolocalisation permanente et géolocalisation sporadique ou géolocalisation de dépistage

Presque tous les types de collecte de données peuvent révéler des détails sur votre emplacement. Vos cartes de crédit, de débit et de fidélité permettent toutes de déterminer votre emplacement à différents moments. Par exemple, si vous utilisez une carte cinq fois dans une journée, un tiers pourrait en apprendre beaucoup sur vos déplacements au cours de cette journée. De plus, après avoir accumulé des données pendant quelques mois, ce tiers pourrait dresser un portrait précis de la distribution spatiale de vos principales habitudes[3]. Les cartes de contrôle d'accès et la biométrie permettent également de localiser une personne et ainsi de suivre ses activités et d'en dresser la cartographie. On appelle ces processus la « géolocalisation ». Or, bien que ces activités soient possibles, il faut faire attention de ne pas assimiler ce qu'il est possible de faire à ce qui se fait concrètement. Il est probable que nombre de ces activités d'analyse *possibles* ne soient pas entreprises ou qu'elles ne puissent être menées à bien à un coût raisonnable.

La surveillance liée à la géolocalisation est toutefois différente des efforts qui consistent à établir un profil géographique en extrapolant à partir

d'autres données. En effet, les dispositifs et techniques de géolocalisation fournissent instantanément des données géographiques qui ne nécessitent pas une analyse de l'exploration de données. Peu importe l'objectif final, une technologie de localisation produit toujours des données géographiques.

Géolocalisation permanente

Pour recevoir des appels, les téléphones portables doivent informer le fournisseur de l'endroit où ils se trouvent en tout temps. Pour ce faire, la plupart des appareils envoient périodiquement un signal aux antennes les plus près. Tous les fournisseurs amassent et conservent ces données pour la facturation, mais aussi à d'autres fins. Ils peuvent notamment utiliser ces données pour dégager des tendances d'utilisation en vue de planifier les futurs besoins en infrastructure. Ils peuvent aussi utiliser ces données à d'autres fins plus nébuleuses. Le petit scandale ayant éclaboussé récemment Apple en est un exemple ; on a dévoilé que les services de localisation intégrés au système d'exploitation des iPhones conservaient l'équivalent d'une année de données dans la mémoire de l'appareil. L'information n'était toutefois pas envoyée aux serveurs d'Apple.

Beaucoup de produits de consommation permettent le suivi géographique en permanence et instantané. À titre d'exemple, les parents peuvent utiliser une balise de radio-identification pour s'assurer que leur enfant ne quitte pas les limites du parc municipal. Un conjoint méfiant pourrait installer discrètement un appareil GPS dans la voiture de son conjoint pour l'espionner. Certains de ces appareils ne font que prélever et enregistrer un échantillon de données sur l'emplacement d'une personne, tandis que d'autres peuvent être interrogés à distance en tout temps pour un contrôle en temps réel. D'ailleurs, les entreprises de location de voitures, les services de partage de voitures et les taxis ont commencé à utiliser ces dispositifs pour gérer leur parc automobile et, le cas échéant, pour veiller à ce que leurs véhicules demeurent dans le périmètre autorisé. Les entreprises de transport commercial ont recours à cette technologie depuis un bon moment, à l'instar des services de police et des services ambulanciers. Dans tous les cas, la gestion du parc automobile est l'objectif premier ; bien entendu, on consigne simultanément des données sur l'endroit où se trouvent les employés et les clients.

Une véritable géolocalisation en permanence est rarement une utilisation efficace des maigres ressources de communication et des ressources informatiques. Souvent, on peut arriver au même résultat en effectuant une

Repérer les téléphones portables (la grande panique iPhone de 2011)

Au printemps 2011, deux passionnés des produits Apple ont remarqué qu'un fichier étrange était synchronisé entre leur iPhone et leur ordinateur. Ils ont alors décidé d'approfondir leur enquête et ont découvert que le fichier était un registre dans lequel était consigné chaque tour de téléphonie cellulaire et chaque point d'accès sans fil auxquels ils s'étaient connectés dans les douze derniers mois. Ces données servent à alimenter les applications géodépendantes, comme FourSquare et, bien sûr, iAd. Les amis ont ensuite conçu une application pour transformer les données brutes de repérage en carte de leurs déplacements. La rumeur s'est alors répandue comme une traînée de poudre sur Internet : Apple fait la poursuite des utilisateurs de iPhone. En réalité, il s'est avéré qu'Apple n'amasse pas les données. Les données de localisation sont seulement consignées dans un fichier (non chiffré) sur le téléphone et sur l'ordinateur personnel des utilisateurs et mis à jour à chaque synchronisation.

Dans les faits, Apple n'a pas besoin de savoir où se trouvent ses clients. L'entreprise utilise ces données géographiques pour transmettre des informations géodépendantes aux utilisateurs, soi-disant pour améliorer leur expérience. Elle en profite également pour maximiser ses revenus en envoyant des publicités pour des entreprises qui sont situées près du téléphone. Apple n'est pas la seule à agir de la sorte. Entre autres, Google Now, l'assistant numérique personnel proposé sur Android, suit également la position de l'utilisateur et offre spontanément des renseignements sur les attraits se trouvant dans l'environnement immédiat lorsqu'il est en mode passif.

Google Now peut également déduire des faits ou la signification des emplacements. À titre d'exemple, l'application peut identifier automatiquement votre maison et votre lieu de travail en fonction des données qu'elle recueille sur vos déplacements habituels. Associé à Google Latitude, ce système permet aux utilisateurs de contrôler et d'adapter le partage de cette information avec leurs « amis » ou avec toute personne qui voudrait connaître leur emplacement.

géolocalisation sporadique, soit en effectuant une collecte intermittente de données à partir d'un appareil. On recueille donc des données importantes ou utiles sans nécessairement dresser un portrait complet des allées et venues de la personne. Comme l'humain a des habitudes bien ancrées, ils suffit d'accumuler des données sporadiquement pendant de courtes périodes de temps, par exemple pendant quelques mois, pour être en mesure de prévoir où se trouvera une personne à un moment donné.



Le iPhone : un dispositif de repérage ? (Source : Wikimedia Commons et carte de l'application Localiser mon iPhone)

Google Glass, le nouveau projet du titan du Web, promet la superposition de certaines données directement dans le champ de vision de la personne qui porte les lunettes spécialement conçues. On appelle souvent cette technique, la « réalité augmentée ». Le profilage et le ciblage des utilisateurs devront être accrus; les lunettes devront choisir minutieusement l'information qui est pertinente afin de ne pas surcharger l'utilisateur d'information et l'obliger à manipuler constamment l'appareil. Chaque demande, qu'elle soit générée par l'utilisateur ou par l'appareil, sera géocodée et liée au compte personnel de l'utilisateur, et ce, pour une durée inconnue.

Géolocalisation sporadique et intermittente

Un appareil GPS enregistre de façon continue sa position pendant que l'appareil est en fonction. C'est notamment le cas des systèmes de navigation GPS installés dans les voitures et les bateaux. Cette localisation est *interne* dans le sens où l'appareil GPS calcule sa propre position et ne communique pas avec un système extérieur. Il n'y a aucun utilisateur tiers. Le propriétaire de l'appareil est le seul à pouvoir voir les données et à surveiller sa position.

La surveillance aux fins de localisation par GPS est généralement sporadique ou intermittente ; c'est-à-dire que l'appareil enregistre des données GPS qui sont consultées ultérieurement . Dans ce cas, un tiers pourrait repérer les déplacements du propriétaire de l'appareil pour une période de temps donnée (en fonction des capacités de l'appareil). Citons comme exemple les dispositifs portatifs de positionnement qu'utilisent les randonneurs et qui permettent d'enregistrer un nombre prédéterminé de positions.

Par ailleurs, on entend par surveillance intermittente, le fait qu'un appareil se connecte automatiquement, de temps à autre, pour donner sa position. La plupart des téléphones portables fonctionnent de cette façon. L'appareil en déplacement se localise approximativement dans les cellules de téléphonie ; il peut également trianguler sa position au moyen des signaux envoyés par plusieurs antennes ou au moyen de l'unité GPS si une position plus précise est requise (et si ces fonctions sont activées). Du point de vue d'un responsable de la surveillance, cette surveillance intermittente présente un désavantage : elle produit d'assez grandes quantités de données-rebuts, soit des renseignements inutiles sur des positions géographiques courantes, constantes ou répétitives. De plus, l'utilisateur d'un téléphone cellulaire peut simplement désactiver le service de géolocalisation et ne laisser que la fonction d'itinérance requise ; cette technique permettrait également de prolonger la durée de vie de la pile. En fait, nombre de téléphones désactivent automatiquement ce service dès que le niveau de la pile est bas. Par conséquent, la surveillance GPS au moyen d'un appareil portable est très peu fiable.

Il existe de nombreux autres exemples de géolocalisation intermittente et de nouvelles technologies qui prennent des échantillons de notre position géographique. À titre d'exemple, certaines cartes pour le transport en commun ou pour les autoroutes à péage enregistrent votre point d'entrée et votre point de sortie pour calculer le tarif que vous devez payer.

Enfin, les données géographiques peuvent également prendre la forme d'une simple trace laissée par une activité qui n'a aucun lien avec celles-ci. Les gazouillis publiés sur Twitter sont notamment géomarqués depuis 2009 ; c'est-à-dire que chaque fois que quelqu'un publie un gazouillis, Twitter consigne de l'information sur l'emplacement géographique de l'appareil utilisé pour créer la publication. Il est donc possible de chercher des gazouillis et de les trier en fonction de l'information sur leur position. Des applications comme Twoogle Geo Search peuvent se servir de ces données pour établir la cartographie des derniers gazouillis publiés près d'un endroit précis sur la planète[4]. Ainsi, il est possible de « suivre » les utilisateurs et le contenu

Société de transport TransLink de Vancouver et la carte Compass

[Traduction] Comment fonctionne la carte Compass? Il suffit de placer la carte près d'un lecteur chaque fois que vous montez dans un autobus ou dans un train West Coast Express, ou que vous arrivez au point d'entrée du SeaBus ou du SkyTrain. Puis, asseyez-vous confortablement et profitez du trajet. N'oubliez pas de présenter de nouveau votre carte en sortant; Compass calculera automatiquement le coût du trajet.

—Description de la carte Compass que l'on trouve sur translink.ca

Les cartes passives d'identification par radiofréquence utilisées pour le transport en commun permettent de situer l'usager à divers points de contrôle à des moments précis. Bien qu'elles ne permettent pas de définir l'emplacement exact ou de transmettre des données en continu, elles peuvent situer approximativement l'usager entre les points de contrôle du trajet.

Le potentiel de surveillance de ces cartes est accru lorsque l'usager doit présenter des documents d'identité au moment d'acheter la carte. Si la carte est anonyme, la base de données n'enregistrera qu'un identifiant unique ainsi qu'un code d'entrée et de sortie. Ces simples données peuvent être recueillies à des fins administratives, notamment afin d'optimiser l'efficacité du système. Pour être plus pratiques ou pour faire réaliser des économies, certaines cartes permettent à l'usager de payer à la fin du trajet. Dans ce cas, l'usager doit ouvrir un compte personnel qui sera associé à son utilisation du transport en commun. La base de données qui en résulte contient des données sur les trajets effectués par tous les usagers inscrits.

La carte Compass à Vancouver est un hybride des deux systèmes. Bien que les usagers n'aient pas à s'inscrire et qu'ils puissent utiliser une carte anonyme, ils peuvent choisir d'associer leur carte à un identifiant; il s'agit là d'une mesure de protection supplémentaire et commode en cas de perte de la carte, pour le renouvellement automatique et pour les reçus à des fins fiscales.

multimédia téléversé qu'ils ont consulté. Les applications rendant ces processus automatiques peuvent dresser rapidement le profil des personnes se trouvant à un endroit en particulier ou faire des recherches pour déterminer l'endroit où des personnes répondant à un profil en particulier se sont rassemblées.

Les photos prises couramment avec un téléphone ou un appareil photo muni d'un GPS peuvent également être assorties de données géographiques.



Trolleybus de TransLink à Vancouver (Source : © Wikimedia Commons/Bobanny, http://commons.wikimedia.org/wiki/File:Vancouver_trolley2101_050720.jpg)

Ce type d'appareils photo enregistrent leur position – et donc celle des personnes figurant sur la photo – au moment où la photo est prise. À titre d'exemple, si on combine ces données avec les nouvelles capacités de reconnaissance faciale de Facebook, il devient possible non seulement d'identifier les gens mais également de les localiser.

Peut-être plus que toute autre forme de données géographiques, l'importance du repérage dépend de la relation de chaque utilisateur avec les

technologies qu'il possède. Pour ceux qui prennent une photo par année ou qui publient un gazouillis par semaine, les traces sont si éloignées qu'elles révèlent très peu d'information. Par contre, pour les utilisateurs de Twitter qui publient plusieurs douzaines de gazouillis par jour, de même que pour les fins palais qui prennent systématiquement des photos de leur repas (qu'ils publient également sur Twitter !), quiconque suit leurs gazouillis pendant une courte période de temps peut prédire où ils se trouvent en tout temps.

Géographie et identité

Dans sa forme la plus véritable, la géolocalisation permet de produire une série de coordonnées géospatiales qui peut servir immédiatement à surveiller ou à trouver des personnes. Citons comme exemple le dispositif Toddler Tag qui permet aux parents de savoir où est leur enfant dans un rayon de 50 mètres ; le système Victoria Tracking permet de faire la même chose partout dans le monde[5]. Le dispositif de localisation Freedom GPS Locator Watch est conçu pour repérer un membre de la famille qui souffrirait de la maladie d'Alzheimer[6]. Les randonneurs qui sont perdus dans les montagnes pourraient avoir recours à une balise individuelle GPS pour obtenir du secours. Dans tous les cas, les données ne concernent que l'emplacement physique. Ces emplacements ont toutefois une signification qui leur est propre.

L'analyse secondaire des données géographiques peut être divisée en trois catégories. La première est la catégorie « géorelationnelle » et se rapporte à la capacité de découvrir qui se trouve au même endroit que vous. Il est maintenant évident que des applications comme Facebook sont le prolongement des réseaux sociaux traditionnellement créés par les gens qui fréquentent les mêmes endroits, appartiennent aux mêmes groupes ou travaillent au même bureau. Voilà pourquoi il semble logique d'aviser ses amis de l'endroit où l'on se trouve. En permettant aux autres de voir notre emplacement, nous favorisons les rencontres physiques et nous ancrons nos réseaux dans la réalité. Si le réseau typiqe s'étendait réellement au monde entier, la probabilité qu'un des membres soit près d'un autre serait extrêmement faible.

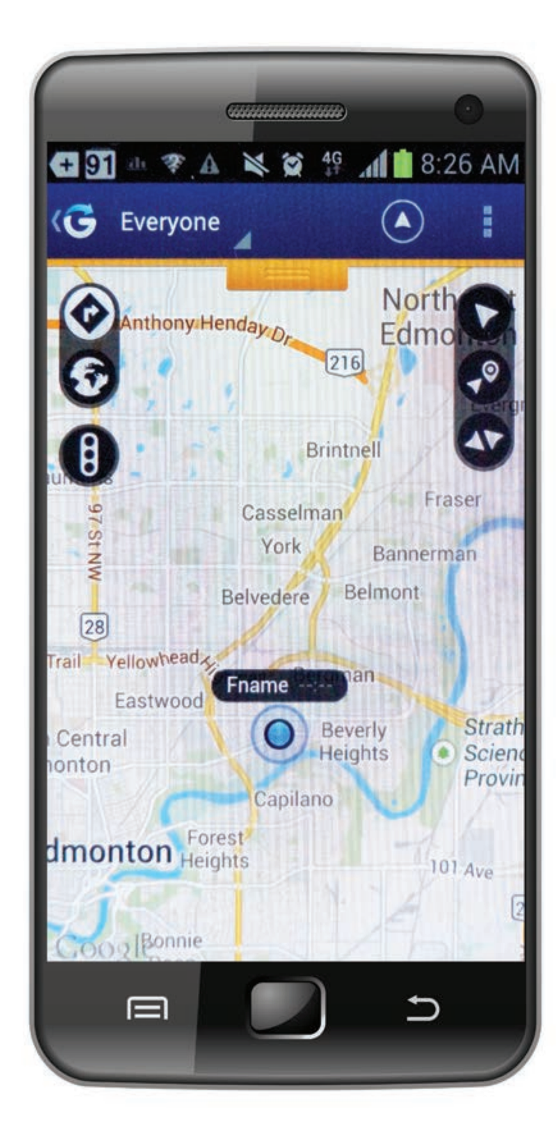
Bien entendu, cela signifie que des tiers peuvent voir avec qui vous êtes et à quel moment. Certaines applications mobiles prennent appui sur ce principe. C'est le cas notamment de la tristement célèbre application Girls

Around Me, qui permettait de voir les profils Facebook des femmes (ou des hommes) qui s'étaient connectées récemment à Foursquare (service mobile géodépendant). C'est le cas également de l'application – moins controversée quant à elle – Banjo qui utilise des capacités beaucoup plus puissantes pour chercher sur presque tous les sites de réseautage social pour trouver les utilisateurs qui se trouveraient à proximité. Il est à noter également que les données géorelationnelles doivent être interprétées en fonction du temps : être avec un collègue à 15 h ne signifie pas la même chose qu'être avec ce même collègue à 3 h. Ces données peuvent également témoigner d'une différence de traitement entre les sexes ; à titre d'exemple, les silhouettes féminines à la James Bond que l'on trouve sur le site Girls Around Me ont suscité un débat houleux sur la représentation de la femme comme une victime ou comme un objet par la technologie[7].

La deuxième catégorie d'analyse des données géograhiques est « géosociale ». Elle consiste à identifier la signification sociale particulière de la position individuelle. Être à la maison n'est pas la même chose qu'être au travail ; se trouver dans un quartier notoire pour la prostitution est différent de se trouver dans le quartier des spectacles. Les données géosociales présentent également une dimension temporelle ; un même emplacement géographique ne signifie pas la même chose selon le moment de la journée. Être à la maison pendant la journée ne signifie pas la même chose qu'être à la maison le soir.

Enfin, dans la troisième catégorie, l'analyse est « géoinformationnelle » ou « géoinformatique ». Dans un avenir rapproché, nous pouvons nous attendre à ce que les données d'Internet soient générées par des réseaux et des sous-réseaux se composant d'humains et de machines. Cette omniprésence de l'informatique signifierait que les machines ne servent plus simplement à transporter ou à stocker du contenu ; elles serviraient également à le comprendre, à le traiter et à en créer. Autrement dit, les machines feront partie du réseau plutôt que d'être un simple outil de communication.

Dans un univers où l'informatique sera omniprésente, le rôle des humains dans le réseau sera transformé de façon imprévisible. Les couches physiques et informatives de l'expérience de l'utilisateur se chevaucheront et se fondront au fur et à mesure que le fossé que nous percevons actuellement entre le monde réel et le monde virtuel se rétrécira. La géolocalisation de tous les objets fera partie intégrante de notre vie quotidienne. D'ailleurs, la majeure partie des technologies nécessaires pour prendre en charge ces avancées existent déjà.



Glympse génèrent des informations de localisation en continu (Source : Google Play)

La géographie dans la pratique

La façon dont les données sont utilisées est un facteur digne d'intérêt dans le cadre de la surveillance de la mobilité. Les données de localisation des téléphones portables sont utilisées immédiatement pour acheminer les appels aux abonnés. Or, lorsque les données de localisation sont utilisées à d'autres fins, elles peuvent entraîner une forme d'intervention qui toucherait

tant les abonnés que les non-abonnés. Souvent, cette intervention s'accompagne d'une classification et d'un tri des personnes en groupes, qui seront ensuite traités différemment. Prenons par exemple les consommateurs à qui l'on accorde une grande ou une faible importance en fonction des endroits qu'ils fréquentent. Les gens qui ont tendance à se trouver souvent dans des zones prospères pourraient bénéficier entre autres d'un accès préférentiel à des articles, des services, des sites, des échantillons prisés. Les policiers commencent à reconnaître l'importance de procéder à de l'exploration de données pour l'information électronique à laquelle ils ont librement accès (qu'on appelle souvent « de source ouverte »). Au fur et à mesure que cette pratique se répandra, certaines séquences et certains déplacements formant des patterns préétablis pourraient être perçus comme suspects et pourraient déclencher une intervention des policiers.

Afin de mieux comprendre les applications concrètes de la géolocalisation, il convient de les diviser en deux catégories non exclusives. La première catégorie comprend les usages internes de la géolocalisation : les utilisateurs enclenchent le processus de localisation qui se présente en soi comme un service. Cette première catégorie s'oppose à la seconde, la géolocalisation externe. Celle-ci s'applique lorsqu'un non-utilisateur – habituellement un fournisseur de services – recueille à ses propres fins les données de localisation d'utilisateurs qui participent à d'autres activités. Cette catégorie implique souvent qu'une personne consent à être surveillée en échange de biens ou de services.

Géolocalisation interne

C'est le consommateur qui est à l'origine de la géolocalisation interne. Mentionnons comme exemple les applications comme Foursquare, qui permettent aux utilisateurs d'indiquer l'endroit où ils se trouvent à leurs amis. Google+ et Facebook offrent également un service de localisation équivalant aux utilisateurs qui souhaitent informer certains groupes de personnes de l'endroit où ils se trouvent. Dans ces cas, les données géographiques ne sont pas une simple monnaie d'échange pour l'obtention d'un autre service ; elles sont la fin en soi.

Bien entendu, la possibilité de publier sur Internet l'endroit où l'on se trouve ne date pas d'hier ; rien n'empêchait les webmestres des premiers sites de mettre à jour leur emplacement. De plus, nombre des premiers blogues indiquaient où se trouvait le blogueur et à quelle heure. La nouveauté,

dans ce qu'il est convenu d'appeler le réseautage géosocial, est que la position de l'utilisateur est perçue comme une partie intégrante de l'expérience de communication avec les autres. On suppose que l'information sur la position est fiable puisqu'elle est générée automatiquement plutôt qu'indiquée par l'utilisateur. Les utilisateurs d'appareils mobiles peuvent tout de même choisir quand dévoiler leur position, mais il est difficile de la contrefaire.

Géolocalisation externe

On dit de la géolocalisation qu'elle est externe lorsque le consommateur n'est pas le bénéficiaire immédiat. Le but principal de la majorité des technologies et des stratégies citées précédemment est de commercialiser des biens, des services et de l'information auprès des utilisateurs. En réalité, presque toutes les applications qui ont la cote actuellement et qui permettent de localiser les utilisateurs sont gratuites, c'est-à-dire que le principal prix à payer est une plus grande exposition aux publicités. Cependant, la ligne entre la publicité et le contenu est devenue si mince que, du point de vue des utilisateurs, elle n'est souvent plus perceptible. Certes, le bandeau publicitaire classique ancré en haut d'une page de contenu et maintenant omniprésent sur YouTube est facile à remarquer – surtout car beaucoup le trouvent franchement énervant. Par ailleurs, une nouvelle série « d'hybrides » est venue effacer la distinction qu'il restait entre le contenu et la publicité. La plateforme iAds d'Apple a notamment été conçue pour que les publicités puissent être visionnées et partagées comme n'importe quel autre contenu. De plus, les mentions « J'aime » sur Facebook servent autant à exprimer l'intérêt des utilisateurs qu'à faire de la publicité. Les fichiers multimédias classiques comme les chansons ou les films sont presque toujours liés à des objectifs de marketing ; on y greffe maintenant des publicités, du placement de produits ou des « offres spéciales ».

Dans ce contexte, on utilise des formes externes de géolocalisation. La nature de plus en plus ciblée de la commercialisation comprend maintenant une dimension de géolocalisation pour deux raisons : tout d'abord, parce que la plupart des affaires sont encore traitées en personne et ensuite parce que la proximité des points de vente est encore vue comme un débouché de taille par les annonceurs et les vendeurs. Les publicités interactives sont plus efficaces si elles ne ciblent pas seulement les utilisateurs en fonction de leurs intérêts, mais également en fonction de leur position dans la ville. À titre d'exemple, Les Restaurants McDonald du Canada Limitée offrent une



Application de McDonald's Canada pour Android (Source : Google Play)

application pour Android et iPhone dont la seule fonction est de trouver ses restaurants au moyen du GPS ou des services de géolocalisation du réseau. Cette application a été téléchargée des milliers de fois par mois depuis son lancement. Elle permet toutefois d'accéder au numéro de série unique du téléphone et au numéro de téléphone de l'utilisateur pour télécharger vers l'amont ou vers l'aval des renseignements non spécifiés vers les serveurs de l'entreprise. Autrement dit, les utilisateurs offrent leur position ainsi que

d'autres données afin que McDonalds puissent leur dire s'ils sont près d'un de ses restaurants.

Nous pouvons par conséquent prédire qu'une géolocalisation de masse se produira non pas *en dépit du* tollé soulevé par les consommateurs, mais bien *parce que* les consommateurs l'ont demandé. La possibilité de troquer notre position pour des biens et des services est déjà perçue comme une nouvelle valeur ajoutée pour une catégorie de renseignements personnels qui autrement semblerait inutile[8]. Par conséquent, à moins que les consommateurs commencent à se demander si cette pratique est contre la loi, l'éthique, le bon sens ou l'intérêt collectif, elle s'effacera progressivement du débat public. Or, pour le moment les consommateurs échangent sans hésiter des parcelles de renseignements personnels contre des biens, des services et de l'information. On nous enseigne à chasser les offres, les aubaines ou les coupons et, pour garantir la valeur, nous cherchons à obtenir l'opinion des autres consommateurs qui y étaient et qui ont vu de leurs propres yeux. Nous devons aussi trouver instantanément la voiture partagée, la station bixi* ou l'arrêt d'autobus le plus près pour réduire notre empreinte environnementale ou le temps perdu. Nombre des propriétaires d'une voiture General Motors sont des abonnés de Onstar (le service de navigation routière) puisqu'ils aiment se sentir plus en sécurité lorsqu'ils sont sur la route. Il semble bien que certains souhaitent connaître le ratio hommes-femmes avant d'entrer dans un bar[9]. Voilà pourquoi selon le site Programmable Web, les interfaces de programmation (API) et les mashups (applications composites qui amalgament le contenu provenant de différentes sources) dans le domaine de la localisation se multiplient à un rythme soutenu (bien sûr à ce stade on assiste à une multiplication de toutes les applications mobiles)[10].

Un autre facteur alimentant l'augmentation du phénomène de la localisation est le désir des industries d'en apprendre davantage sur les consommateurs afin de produire et de mettre en marché des biens et des services. Dans ce cas, ce n'est pas la proximité des clients aux entreprises qui compte ; c'est plutôt la signification de la distribution géographique de leurs comportements. À titre d'exemple, Amazon pourrait vouloir savoir où vous êtes afin de pouvoir vous offrir un livre sur cet endroit.

* Système de vélos libre-service mis en place par la Ville de Montréal. L'application mobile permet de connaître, en temps réel, le nombre de vélos et de points d'ancrage disponibles à chaque station.

Le même type d'information peut être utilisé pour faciliter la gestion et l'entretien d'infrastructure matérielle, telle que des routes et des autoroutes. Ce type de surveillance est déjà utilisé dans la région du Grand Toronto, notamment pour l'autoroute à péage électronique 407 (ETR407) et sur le nouveau pont Port Mann qui relie Coquitlam à Surrey. Sur cette autoroute et ce pont, de l'information sur le point d'entrée et le point de sortie des automobilistes est utilisée pour facturer les clients. Le système pourrait dans l'avenir avoir recours à des taux variables pour réduire la congestion comme nombre d'autres villes le font. Toronto utilise sur l'ETR407 des transpondeurs spéciaux installés sur le pare-brise, de même qu'un système de reconnaissance automatique des plaques d'immatriculation (*automated licence plate recognition*, ALPR). Cest le système qui s'est répandu le plus rapidement parmi tous les systèmes contemporains. Il est utilisé par les caméras automatisées de régulation de la circulation, par les caméras installées sur les voitures des policiers, par les systèmes automatisés d'exploitation des parcs de stationnement et bien d'autres. Il sert également à l'application des politiques environnementales qui prévoient la circulation d'un nombre limité de voitures dans un centre-ville ou à l'exécution d'initiatives de sécurité. Jusqu'à maintenant, la plupart des systèmes de reconnaissance automatique du numéro d'immatriculation nécessitent l'installation de caméras spécialement conçues. Toutefois, de nouveaux logiciels permettent l'analyse de grandes quantités de données et la recherche de numéro d'immatriculation dans des vidéos préenregistrées ou des banques d'images.

Du moment où des pistes de géolocalisation sont offertes ou peuvent être extraites d'autres systèmes, comme des caméras municipales de surveillance de la circulation munies d'un dispositif de reconnaissance des visages, des vêtements ou des objets ; d'un logiciel de reconnaissance des plaques d'immatriculation ; ou de cartes personnalisées pour le transport en commun, nous pouvons nous attendre à voir une avalanche de dispositifs et d'applications de géolocalisation. Il devient alors possible de reconnaître et de suivre automatiquement des citoyens, même s'ils ne sont pas identifiés. Des interventions très personnalisées pourront être effectuées, que ce soit à des fins de contrôle social, de commercialisation, de sécurité, de divertissement ou d'application du principe de l'utilisateur-payeur et, bien entendu, pour la filature, pour satisfaire sa curiosité ou pour faire du chantage.

Conclusion

Bien que toutes les nouveautés présentées précédemment existent et soient utilisées couramment de nos jours, l'engouement entourant réellement les applications géodépendantes est parfois exagéré[11]. Très peu de services géodépendants sont parvenus à prendre pied sur le marché ; le pourcentage est bien inférieur à 10 % aux États-Unis[12]. Néanmoins, nombre de ces technologies ont été mises au point depuis peu et il est très probable qu'elles progressent dans l'avenir.

Prenons un autre exemple pour bien distinguer l'essentiel de la situation. Bien que la sécurité automobile et routière soit une préoccupation sociale de premier plan, le public demeure réticent à accepter des nouvelles technologies de sécurité routière, comme les caméras de contrôle de la vitesse. Des enregistreurs de données routières (communément appelés EDR ou « boîte noire ») sont installés sur certaines voitures pour enregistrer des renseignements lors de collisions ou d'accidents. Malgré leurs capacités techniques, les EDR sont rarement utilisés et sont mêlés au débat sur la protection de la vie privée. D'ailleurs, la National Highway Traffic Safety Administration (NHTSA) aux États-Unis fait un « examen » des normes relatives aux enregistreurs de données routières depuis 2005. Même si de formidables projets de systèmes de transport intelligent[13] sont en cours de réalisation, il est difficile de croire qu'ils pourraient être mis en œuvre à court ou à moyen terme ; ces systèmes de transport intelligent permettraient aux voitures de communiquer entre elles ainsi qu'avec des systèmes de régulation de la circulation. Outre leurs limites technologiques, les craintes concernant ces technologies portent sur leurs coûts nets pour les citoyens en termes de perte de liberté.

Autre aspect à noter : pour les technologies décrites précédemment, les particuliers ne sont presque jamais localisés ; on localise plutôt les appareils, que ce soit les téléphones portables, les étiquettes d'identification par radiofréquence ou les transpondeurs. On doit toujours avoir foi que le propriétaire identifié a en sa possession l'appareil. Cette foi doit être d'autant plus grande si le repérage est rare ou intermittent, avec une marge d'erreur élevée. Par ailleurs, on ne peut éviter qu'une personne tente de tromper ces systèmes ou se montre plus maligne qu'eux lorsqu'il est à son avantage de le faire. Prenons par exemple les quelques caméras de contrôle de la vitesse installées au Québec (15 emplacements) qui ont déjà incité certaines personnes à employer de faux numéros d'immatriculation.

Il existe deux façons de réagir à ces sources d'incertitude. La première consiste à augmenter le suivi jusqu'au point où suffisamment de données sont recueillies pour établir un profil individuel identifiable. Cette intervention ne requiert pas un suivi complet et continu. Les profils établis avec moins de données assurent avec une exactitude presque parfaite que la même personne a en sa possession l'appareil. Toutefois, cette personne pourrait ne pas être le propriétaire officiel ou enregistré de l'appareil ou celle dont le nom figure sur le contrat.

La seconde réaction serait de remplacer le numéro d'identification unique de l'appareil par la biométrie. On pourrait ainsi établir un lien direct entre les données de géolocalisation et les personnes plutôt qu'entre les données et l'appareil. Il est déjà fréquent de voir des ordinateurs portables munis d'un lecteur d'empreintes digitales qui permet de verrouiller l'ordinateur et de protéger les données sensibles du propriétaire. Depuis des années, Microsoft offre dans son système d'exploitation Windows une version chancelante du verrouillage électronique au moyen des empreintes digitales. Les fabricants commencent également à installer la technologie de reconnaissance des empreintes digitales sur les téléphones intelligents et les tablettes. De plus, certains téléphones intelligents sont déjà dotés d'une technologie de reconnaissance faciale pour le verrouillage ; dans ce cas il est connu par contre qu'une simple photo peut tromper cette technologie. La prochaine génération d'écrans tactiles prendra en charge la biométrie, c'est-à-dire qu'elle fera une lecture en continu des empreintes digitales lorsque l'utilisateur se servira du téléphone ou de la tablette. Les empreintes digitales ne serviront plus seulement à déverrouiller l'appareil et les changements d'utilisateurs seront détectés. Si nous projetons ces technologies de biométrie et de géolocalisation un peu plus loin dans le futur, nous pouvons imaginer que les nouvelles technologies, comme les lunettes Google, ne reconnaîtront pas seulement l'utilisateur au moyen de la reconnaissance de l'iris, mais également les personnes qui l'entourent, qu'elles en soient conscientes ou non, et qu'elles y consentent ou non.

Notes

1 Anna Klimaszewski-Patterson, « Smartphones in the Field: Preliminary Study Comparing GPS Capabilities Between a Smartphone and Dedicated GPS Device », *Papers of the Applied Geography Conferences* -59 (2010), p. 178-371, http://www.academia.edu/353833/Geographic_Fieldwork_Preliminary_study_comparing_GPS_capabilities_between_smartphones_and_dedicated_GPS.

2 Online Publishers Association, *A Portrait of Today's Tablet User Wave II,* juin 1920, http://www.atelier.net/sites/default/files/etude/utilisateurs_americains_de_tablettes.pdf.

3 Daniel Ashbrook et Thad Starner, « Using GPS to Learn Significant Locations and Predict Movement Across Multiple Users », *Personal Ubiquitous Computing* -85 (1911), p. 183-378.

4 Voir Twoogle Geo Search, http://twoogle.co.uk/.

5 Pour un exemple de balise GPS pour enfants, voir http://www.brickhousesecurity.com/product/toddler+tag+child+locator.do; pour une description du Victoria Tracking Service, système de repérage GPS pour enfants, voir http://www.tracking-system.com/for-consumers/gps-tracking-children.html.

6 Voir Freedom GPS Locator Watch de Bluewater Security Professionals, LLC, (montre GPS de repérage pour les personnes âgées, les personnes souffrant de la maladie d'Alzheimer ou de démence), http://www.bluewatersecurityprofessionals.com/elderlytracking.htm.

7 Voir Kashmir Hill, « The Reaction to 'Girls Around Me' Was Far More Disturbing Than the 'Creepy' App Itself », *Forbes*, 2 avril 2012, http://www.forbes.com/sites/kashmirhill/2012/04/02/the-reaction-to-girls-around-me-was-far-more-disturbing-than-the-creepy-app-itself/.

8 Stéphane Leman-Langlois, « Privacy as Currency: Behaviour Control in the Industrial Cyberspace », dans Stéphane Leman-Langlois (dir.), *Technocrime: Technology, Crime and Social Control* (Cullompton, Royaume-Uni, Willan Publishing, 1916), p. 20-230.

9 Voir scenetap.com, « SceneTap lets you check out the scene in real-time ».

10 Janice Y. Tasi, Patrick Gage Kelley, Lorrie Faith Cranor et Norman Sadeh, « Location-Sharing Technologies: Privacy Risks and Controls », *I/S: A Journal of Law and Policy for the Information Society* 6, nº 2 (2010), p. 119-152.

11 Voir Mohamed Kahlain, « Location Based Segmentation in Canada », *Mediative Blog: The Digital Results People*, 19 janvier 2012, http://blog.mediative.com/en/2012/01/19/location-based-marketing-segmention-canada/.

12 Voir Kathryn Zickuhr et Aaron Smith, « 4% of Online Americans Use Location-Based Services », *Pew Internet*, 4 novembre 2010, http://www.pewinternet.org/Reports/2010/Location-based-services.aspx.

13 Pour plus de renseignements sur les systèmes de transport intelligents, voir Ching-HungYeh, Yueh-Min Huang, Tzone-I Wang et Hsiao-Hwa Chen, « DESCV-A Secure Wireless Communication Scheme for Vehicle ad hoc Networking », *Mobile Networking Applications* -78 (2009), p. 519-716.



Mondialisation de la surveillance

De national à mondial

L'expression « surveillance mondiale » évoque dans l'imaginaire l'espionnage international, les tentacules des services de renseignements clandestins qui s'étendent partout dans le monde, comme la trame d'un roman à suspense. De façon plus réaliste, elle renvoie également à des organismes comme la National Security Agency (NSA) aux États-Unis. Une telle surveillance mondiale existe bel et bien, mais nous utilisons l'expression surtout pour nous rapporter, de manière plus terre à terre, à des phénomènes comme l'apparition de normes internationales pour la sécurité dans les aéroports ou l'étiquetage des biens de consommation au moyen de codes uniformisés. Vos lames de rasoir ou votre chemise pourraient contenir une étiquette d'identification par radiofréquence conforme à un code électronique de produit universel et associée à un système mondial de synchronisation des données. Mais ces termes techniques ont peu d'importance. Il faut plutôt s'attarder à ce sur quoi ils attirent l'attention : un monde où les liens entre les données permettent à la fois de localiser le fabricant des lames de rasoir ou de la chemise, et de renvoyer à la personne qui les utilise actuellement.

Des processus qui autrefois étaient séparés par les frontières nationales sont de plus en plus connectés au-delà des frontières. La « mondialisation de la surveillance » se rapporte donc à une nouvelle réalité : l'information qui autrefois était cloisonnée par pays est maintenant en format numérique et est ainsi acheminée plus facilement d'un côté à l'autre des frontières. Une

Des données qui transcendent les frontières

Même la commissaire à la protection de la vie privée du Canada s'est heurtée à des problèmes lorsque ses données personnelles ont été communiquées à l'étranger. Il y a quelques années, la revue *Maclean's* a acheté le registre téléphonique personnel de Jennifer Stoddart d'un courtier en données des États-Unis, sans qu'aucune question ne soit posée. À sa grande consternation, des listes détaillées des appels faits de sa maison à Montréal, de son chalet dans les Cantons de l'Est et de son BlackBerry fourni par le gouvernement ont été déposées sur son bureau. On pouvait, entre autres, y voir des appels à un membre de sa famille à Frelighsburg, au Québec, et à la maison de l'un de ses conseillers en communication; la date et l'heure de tous ces appels étaient exactes[1].

Les courtiers en données se présentent sous toutes les formes et les tailles imaginables; de géants comme Acxiom (mentionné dans la Tendance 1) ou Experian, aux plus petits comme InfoCanada. Ils vendent des renseignements personnels obtenus des consommateurs et ils achètent et vendent ces renseignements essentiellement à des fins de marketing. Néanmoins, il arrive que des ministères, des services de police et des services de renseignements aient également recours à leurs services. Comme les régimes juridiques diffèrent – notamment entre le

personne peut par exemple utiliser une carte de crédit dans différents pays et, par le fait même, transmettre les renseignements personnels qui sont liés à ce type de transaction. Par ailleurs, nous connaissons mieux ces liens et ces flux de données. Nous nous attendons à nous soumettre à des mesures de sécurité similaires dans les aéroports du monde entier et à ce que notre passeport puisse être lu par une machine dans n'importe quel aéroport. Ces lecteurs reconnaissent nos données d'identification même si le pays dans lequel nous nous trouvons est loin du nôtre tant sur le plan géographique que culturel.

Les grandes tendances observées à l'échelle mondiale ont une influence considérable sur la surveillance au Canada. Il est évident que la politique et les politiques aux États-Unis sont une source d'influence, mais les ramifications de la surveillance mondiale s'étendent bien plus loin. Ces influences mondiales peuvent prendre la forme d'efforts subtils pour orienter les politiques, d'un partage d'expertise ou de la conformité aux normes et règlements internationaux. Prenons par exemple, la signature par le Canada en 2007 d'un accord de « coopération » en matière de sécurité publique avec

Canada et les États-Unis –, il est difficile de déterminer de quelle compétence relèvent les données personnelles qui circulent maintenant entre les pays et ailleurs.

Pendant des années, les sociétés de courtage de données ont été traitées avec douceur au Canada. Cependant, en 2013, un comité de la Chambre des communes a exhorté le Commissariat à la protection de la vie privée du Canada à rédiger des lignes directrices sur la collecte et l'utilisation de renseignements personnels par les courtiers en données et les médias sociaux[2]. Or, des entreprises comme Facebook et Twitter ne proviennent pas du Canada, à l'instar de nombre d'autres sociétés de courtage de données qui traitent néanmoins des données canadiennes. Le Comité souhaite qu'au moins les données personnelles canadiennes soient mieux protégées. Toutefois, plusieurs députés ont exprimé avec force que les recommandations du Comité sont tout à fait insuffisantes.

1. Jonathon Gatehouse, « You Are Exposed », *Maclean's*, 21 novembre 2005, http://www.macleans.ca/canada/national/article.jsp?content=20051121_115779_115779.
2. Canada, Parlement, *Protection de la vie privée et médias sociaux à l'ère des mégadonnées; Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique* (Ottawa, Parlement du Canada, avril 2013), http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6094136&Mode=1&Parl=41&Ses=1&Language=F.

Israël[1]. Comme Sécurité publique Canada travaille de concert avec l'Agence des services frontaliers du Canada (ASFC), la Gendarmerie royale du Canada (GRC), le Service canadien du renseignement de sécurité (SCRS) et le Service correctionnel du Canada (SCC), les pratiques de surveillance se doivent d'être à la base de cet accord international. Si les services de sécurité israéliens ont recours au profilage racial[2], le Canada devra-t-il lui aussi employer ces techniques discriminatoires à ses frontières ? Qu'importe les détails de l'accord, pour évaluer la dynamique actuelle et future de la surveillance au Canada, on doit examiner le Canada dans le contexte de la mondialisation.

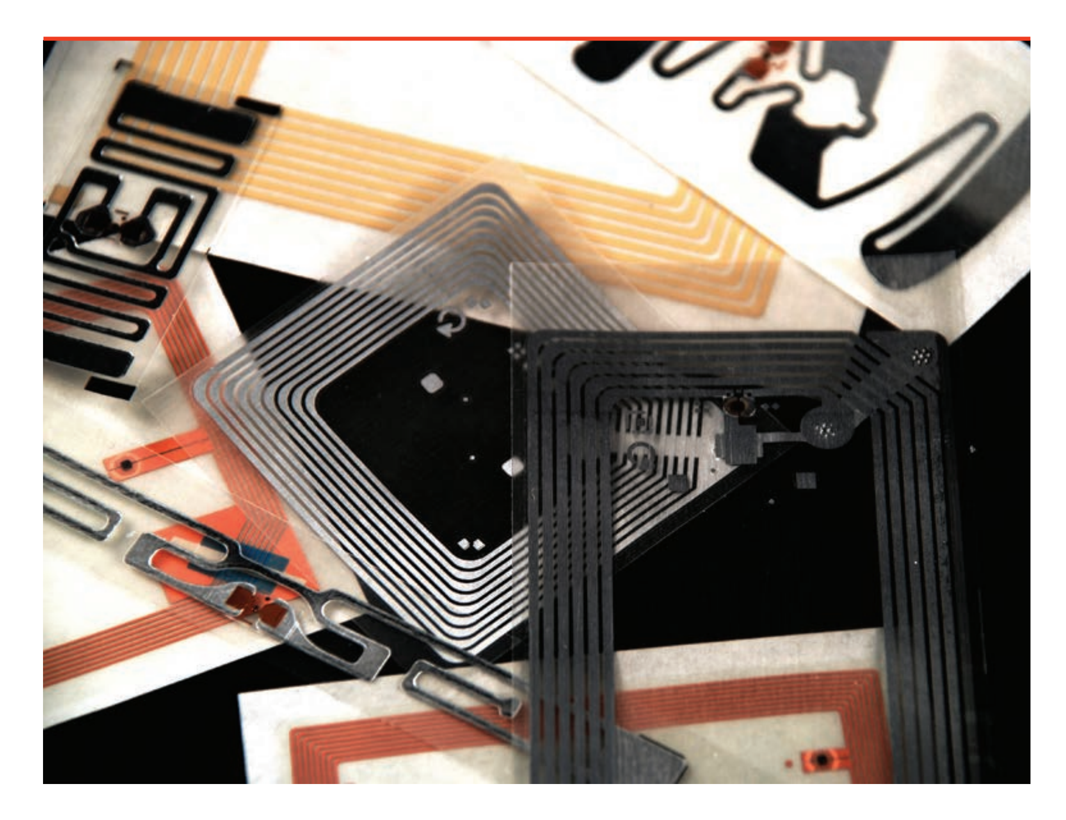
La mondialisation influe grandement sur la surveillance. Il y a autant de chances qu'une personne soit observée par une caméra de surveillance à Toronto, à Johannesburg ou à Tokyo. Les cartes d'identité nationales sont utilisées tant aux Pays-Bas, qu'en Inde et au Brésil. Or, l'enjeu ne réside pas simplement dans l'utilisation de technologies similaires ou dans le fait que les entreprises spécialisées en technologie mènent leurs activités dans différents pays ; on doit également tenir compte du fait que les processus et

Les étiquettes d’identification par radiofréquence permettraient un traçage mondial

Les passeports canadiens et d’autres pays sont maintenant munis d’étiquettes d’identification par radiofréquence qui facilitent la circulation des données personnelles entre les frontières. Les grands voyageurs pourraient toutefois bientôt apprendre à mieux connaître l’identification par radiofréquence pour d’autres raisons. En effet, elle est également incorporée à de nombreux produits de consommation, comme les vêtements, de sorte que nous pourrions involontairement porter des vêtements qui pourraient être balayés pour obtenir des données. Les hôtels utilisent l’identification par radiofréquence pour faire le suivi des serviettes et des robes de chambre et les centres de ski l’utilisent au lieu de laissez-passer de papier pour permettre aux skieurs d’accéder aux remonte-pentes et parfois au bar d’après-ski. Certaines entreprises de location de voitures fournissent à leurs clients des étiquettes d’identification par radiofréquence plutôt que des clés. Enfin, vous pouvez également acheter des biens avec une carte de crédit sans contact, qui utilise également l’identification par radiofréquence.

Bien qu’elles soient minuscules et discrètes, les étiquettes d’identification par radiofréquence promettent d’excellents avantages aux organisations et aux entreprises qui les utilisent, en raison des détails subtils qu’elles fournissent. En effet, l’un des risques associés à cette technologie est que les opinions des citoyens et des organismes inquiets pourraient se noyer dans le discours des parties intéressées[1]. Les étiquettes d’identification par radiofréquence se transforment rapidement en une source de plus en plus importante de « big data », les données volumineuses qui nécessitent des modes nouveaux de gestion et d’analyse. Les gouvernements et les entreprises cherchent de plus en plus à obtenir ces données, parfois à des fins honorables, parfois à des fins moins honorables.

Ceux qui croient que l’identification par radiofréquence et les données volumineuses créeront un système de surveillance mondiale intégré exagèrent parfois les risques pour la vie privée qu’elles représentent. Le Bureau de la consommation fait toutefois cette mise en garde appropriée sur son site Web : « [la technologie d’identification par radiofréquence] permettra d’accroître la localisation secrète et systématique des personnes à une échelle encore plus grande. Cela aura une incidence considérable sur les attentes raisonnables traditionnelles des personnes à l’égard de la protection de la vie privée dans leurs déplacements : elles pourraient avoir été vues



Les étiquettes d'identification par radiofréquence ont plusieurs formes et tailles (Source : © iStock-photo.com/albln)

à une certaine heure à un certain endroit, mais beaucoup moins identifiable pendant une plus longue période. Le résultat global est qu'une plus grande partie de nos vies, dans de plus nombreux endroits, est exposée »[2].

Ainsi, nous vivons à nu non seulement au Canada, mais aussi dans le monde entier.

1. Armand Mattelart, *The Globalization of Surveillance* (Cambridge, Royaume-Uni, Polity Press, 2010), p. 190-193.
2. Industrie Canada, *Les technologies RFID et les consommateurs sur le marché de la vente au détail*, Le Bureau de la consommation, http://www.ic.gc.ca/eic/site/oca-bc.nsf/fra/ca02287.html.

les procédures de surveillance se ressemblent de plus en plus. Peu importe le pays dans lequel vous voyagez, vous devrez sans doute répondre à des questions similaires et vous soumettre à des vérifications semblables à la frontière. Il est aussi fréquent que les processus internationaux soient reliés à des réseaux qui diffusent les renseignements à l'échelle mondiale. Les guichets automatiques bancaires sont un exemple de ces systèmes.

Par ailleurs, la mondialisation de la surveillance n'est pas un processus achevé ; il s'agit d'un phénomène en constante évolution. Toutefois, cela ne signifie pas que les mêmes pratiques de surveillance sont employées dans tous les pays, même si nombre d'entre elles sont couramment utilisées. D'ailleurs, ce n'est pas parce que des caméras de surveillance sont installées dans différentes villes partout sur la planète qu'elles servent nécessairement à effectuer le même type de surveillance. Les systèmes peuvent varier en fonction des groupes de personnes surveillées, de même qu'en fonction des raisons sous-jacentes à cette surveillance. De plus, les systèmes ne font pas systématiquement intervenir un superviseur humain ; les caméras enregistrent souvent des images sans supervision et sont de plus en plus surveillées par des logiciels automatiques.

Malgré les similarités courantes de la surveillance effectuée partout sur la planète, les réseaux qui relient les systèmes de surveillance ne s'étendent pas nécessairement à l'échelle mondiale. Ils peuvent être des réseaux locaux qui ont été mis en place pour répondre à un objectif local. Londres, en Angleterre, est la ville qui affiche la plus grande densité de caméras de surveillance dans le monde. Dans cette ville, deux caméras l'une à côté de l'autre peuvent faire partie de deux systèmes entièrement différents appartenant à des autorités locales ou à des services de police différents. Si l'on essayait de connecter ces deux caméras, on constaterait qu'elles sont incompatibles : certaines sont analogiques et enregistrent en format VHS, d'autres sont numériques et sont connectées par câble, tandis que d'autres transmettent l'information par un réseau sans fil. De la même façon, certaines caméras sont surveillées par un préposé dans une salle de contrôle qui est reliée au service de police tandis que d'autres ne sont surveillées que sporadiquement, d'autres ne font qu'enregistrer ; d'autres encore font partie de réseaux de fausses caméras de surveillance. Il n'existe pas de système unique qui puisse traiter les images des caméras de surveillance à Londres, encore moins celles qui sont captées autour du monde, bien que les experts en sécurité souhaitent aller dans cette direction.

Ces différences sont toutefois compatibles avec la mondialisation puisque mondialisation n'est pas synonyme d'homogénéité. Pour bien définir la mondialisation de la surveillance, on doit reconnaître tant les similitudes que les différences des modes de surveillance utilisés partout dans le monde : les frontières et la culture du pays sont des facteurs qui entrent encore en jeu aujourd'hui. Le Canada ne représente qu'une forme de société de surveillance. La Chine, par exemple, a adopté une forme de surveillance totalitaire qui est, à toutes fins utiles, compatible avec le développement économique capitaliste, même si cette surveillance intensive des opinions politiques et culturelles en Chine peut se répercuter sur la dignité et les libertés individuelles ainsi que sur les possibilités qui se présenteront dans la vie d'une personne. On note également d'importantes différences entre les pays de l'Occident. En effet, certains pays d'Europe, tels que l'Allemagne, ont conféré des droits constitutionnels aux citoyens, ce qui rend plus complexe l'exercice d'une surveillance assujettie à la technologie. À l'opposé, la Suède traite la grande quantité de renseignements personnels amassés par l'État, notamment les données provenant des déclarations de revenus, comme un bien public et permet donc au public d'y accéder. Dans des pays qui connaissent un développement économique rapide comme le Brésil et le Mexique, il est normal que les biens nantis rejettent les protections restreintes offertes par l'État et fassent appel à des services de sécurité privés et à des fournisseurs de service de surveillance. De même, les moins bien nantis sont laissés sans surveillance et sans défense à moins qu'ils se tournent vers l'un des nombreux gangs qui sont à l'origine des craintes des mieux nantis.

Processus de mondialisation

Il existe de nombreux processus de mondialisation, c'est-à-dire que les différents processus et les diverses pratiques, politiques et technologies sont mondialisées de différentes façons et à un rythme différent. Ces formes de mondialisation qui sont liées à la surveillance sont classées en quatre catégories interreliées : mondialisation des intérêts régionaux, mondialisation de la gouvernance, mondialisation des normes et mondialisation des technologies.

Mondialisation des intérêts régionaux

Les satellites artificiels mis sur orbite autour de la terre sont parmi les systèmes de surveillance qui offrent la plus grande couverture mondiale. La plupart de ces satellites sont téléguidés par des organisations militaires, notamment par l'armée étatsunienne. Vers la fin de la Guerre froide, les États-Unis sont parvenus à obtenir le contrôle de l'espace orbital et ont ainsi obtenu l'avantage. La Maison Blanche s'est depuis arrogée le pouvoir de refuser l'accès à l'espace orbital à d'autres pays, si l'État juge que l'utilisation qu'ils en feront menacera ses intérêts. Alors, bien que la portée de la surveillance par satellite semble mondiale, elle servirait plutôt des intérêts régionaux. Autrement dit, dans ce cas on entend par « mondialisation » la mondialisation de la puissance militaire des États-Unis.

La domination des États-Unis s'observe également pour les communications mondiales. L'Internet – une invention de l'armée américaine lors de la guerre froide – avait été conçu initialement comme un outil de communication autoréparant. Si la guerre en venait à détruire tous les autres moyens de communication, l'Internet pourrait se rediriger et éviter les dommages. Aujourd'hui, il est encore administré en majeure partie à partir des États-Unis. La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), qui est l'organisme qui décide comment les noms de domaine et les adresses sont attribués aux pays et autres entités, en est un autre exemple de premier plan. L'Internet, comme les autres systèmes de communication, a amené de nouvelles libertés et de nouveaux moyens de partage et d'organisation pour la population. Ses protocoles dépendent cependant du triage et de la catégorisation automatiques d'immenses quantités de données. On pourrait penser qu'il est impossible d'administrer toutes ces données, mais le volume n'est qu'un problème technique. Les services de renseignements des États-Unis, en particulier la National Security Agency (NSA), par l'intermédiaire du réseau ECHELON et du système PRISM, peuvent utiliser des moyens détournés pour avoir accès aux périphériques et aux logiciels de communications pour intercepter et passer au crible les communications mondiales effectuées par Internet, courriel, téléphone, télécopieur et telex*.

* « ECHELON » était l'un des noms de code utilisés dans le cadre d'une vaste série de systèmes dont la NSA se servait pour intercepter et analyser les communications dans les années 1980 ; depuis que le système a été rendu public, les journaux ont continué d'utiliser ce nom pour désigner le système dans son ensemble.

Bien que d'autres pays exercent une surveillance et un contrôle sur Internet et, à l'instar de la Chine ou de l'Iran, puissent y parvenir efficacement à l'intérieur de leurs frontières, ces pays n'ont pas la portée mondiale qu'ont les États-Unis. Les Étatsuniens ont obtenu ce contrôle en partie en mobilisant des alliés pour l'application de leurs pratiques de surveillance. Par exemple, le Centre de la sécurité des télécommunications Canada (CSTC) est un des partenaires principaux de l'Accord Canada-États-Unis secret de 1948 qui est à la base d'ECHELON[3].

Mondialisation de la gouvernance

Nombre d'activités de surveillance sont exercées à l'échelle mondiale par des institutions comme l'Organisation mondiale de la Santé, la Banque mondiale et le Fonds monétaire international (FMI). Le mandat de ces institutions consiste essentiellement à surveiller les flux d'information dans un éventail de domaines allant de l'économie à l'environnement. Certains de ces systèmes de surveillance, particulièrement ceux portant sur la dégradation de l'environnement ou les épidémies humaines ou agricoles, offrent des bienfaits d'intérêt public. Dans d'autres domaines, ces bienfaits sont par contre plus discutables. Une grande partie de la surveillance effectuée de nos jours a pour objet de protéger des intérêts commerciaux ou de faire progresser la mondialisation du capitalisme.

Les organismes qui mènent des activités à l'échelle mondiale, comme le FMI, ont un mandat clair de surveillance et leurs opérations changent la destinée de millions de personnes. Prenons comme exemple les ajustements structurels auxquels un pays doit procéder pour répondre au critères de stabilité économique du FMI. Jusqu'à récemment, il s'agissait surtout d'imposer le modèle économique anglo-américain aux pays coloniaux émergents (bien qu'exceptionnellement le Royaume-Uni dut apporter des ajustements structurels de ce genre à la suite du ralentissement économique mondial des années 1970). Cependant, tout récemment le FMI imposait à la Grèce et à l'Italie des conditions sévères en échange d'un renflouement, en plus du remplacement des gouvernements élus démocratiquement par des technocrates approuvés par le FMI pour administrer la reprise économique espérée. Dans l'économie mondiale, le contrôle se traduit souvent à l'échelle nationale par un octroi du crédit puis par la surveillance de presque tous les aspects de l'économie de l'État en vue non seulement de favoriser le remboursement,

La poursuite de la NSA va bien au-delà des frontières américaines

Des révélations ont commencé à éclabousser les programmes secrets de surveillance des États-Unis en juin 2013. Accablées, les autorités étatsuniennes ont immédiatement licencié la personne qui a tiré la sonnette d'alarme, Edward Snowden. Elles l'ont accusé de vol, de divulgation d'information de la défense et d'espionnage. L'accusé a notamment révélé que la National Security Authority (NSA) recueille les données téléphoniques de millions de citoyens américains auprès d'entreprises de télécommunications comme Verizon. Il a également levé le voile sur l'existence du système appelé PRISM, lequel donne accès à la NSA et au FBI aux données détenues par des entreprises comme Google, Yahoo, Apple, Microsoft et Facebook. PRISM suit les ressortissants étrangers à l'extérieur des États-Unis. On ne peut donc plus nier la dimension mondiale de ce système qui, comme il se présente, est devenu très irritant pour nombre de pays.

Bon nombre de personnes soupçonnaient depuis longtemps l'existence de tels programmes, mais les preuves directes que Snowden a donné au journal britannique *The Guardian* ont soulevé une intense controverse. Les autorités américaines ont tenté de diminuer l'importance des métadonnées téléphoniques glanées, lesquelles ne visent pas le contenu des communications en tant que tel. Elles ont insisté sur le fait que leur objectif était d'analyser les structures numériques pour cartographier les réseaux terroristes et non pas de procéder à une surveillance de masse. Or, les métadonnées révèlent qui a parlé avec qui, l'endroit où les interlocuteurs se trouvaient et bien d'autres détails desquels on peut glaner les préférences et priorités politiques et personnelles. La collecte de ces données peut sembler mineure et sans intérêt. Cependant, comme le suggère Daniel Solove, ces données sont comme un tableau de Georges Seurat : si l'on regroupe chaque élément de métadonnées, on obtient une image qui se rapprocherait davantage d'une information que d'une simple donnée[1].

Manifestement, tant les métadonnées que le contenu intégral des messages sont capturés par PRISM, et les courriels ou les messages sur les sites de clavardage sont traités par des sociétés étatsuniennes, qu'ils quittent le Canada ou non. Par conséquent, à l'instar des ressortissants

mais également de veiller à ce que le pays se conforme aux normes de concurrence économique internationale.

Ces pratiques sont semblables à la façon dont les banques et les institutions financières utilisent l'information amassée au moyen de la



Caches de données de surveillance planétaire qu'utilise la NSA pour stocker les données amassées par PRISM et probablement par d'autres programmes d'interception des communications (Source : Glenn Greenwald, « XKeyscore: NSA Tool Collects Nearly Everything a User Does on the Internet », *The Guardian*, Royaume-Uni, 31 juillet 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data *[en anglais seulement]*)

étrangers à l'extérieur des États-Unis, les Canadiens sont évidemment vulnérables au suivi des données personnelles fait par les États-Unis. Alors, est-ce que cela signifie que des organismes canadiens comme le Centre de la sécurité des télécommunications Canada (CSTC) collaborent avec le programme PRISM ou avec d'autres programmes similaires? Il est fort probable que ce soit le cas, selon le chroniqueur en matière de droit et de technologie, Michael Geist[2]. Toutefois, étant donné le secret entourant le CSTC, il est difficile de le savoir réellement. Une telle mondialisation de données personnelles hautement significatives nécessite une supervision plus rigoureuse, affirme Jennifer Stoddart, commissaire sortante à la protection de la vie privée du Canada, et ce, tant au Canada qu'aux États-Unis[3]. Nombre de citoyens partout dans le monde sont du même avis.

1. « Surveillance: A Threat to Democracy », éditorial, *New York Times*, 11 juin 2013, http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?_r=1&.
2. Michael Geist, « Why Canadians Should Be Demanding Answers About Secret Surveillance Programs », billet sur le blogue, 8 juin 2013, www.michaelgeist.ca/content/view/6869/125/.
3. Jennifer Stoddart, *Vers une réglementation internationale de la vie privée : propositions et stratégies*, allocution lors de la 31e Conférence internationale des commissaires à la protection des données et de la vie privée, Madrid, 6 novembre 2009, http://www.priv.gc.ca/media/sp-d/2009/sp-d_20091106_f.asp.

surveillance pour prendre des décisions quant aux services qu'elles offrent à leurs clients. Parmi ces renseignements, mentionnons les données personnelles et financières du client recueillies par la banque ou par des agences de notation externes et les renseignements moins « objectifs » glanés au

cours des entrevues et des réunions. En combinant les données de différentes sources, les banques et les institutions financières peuvent établir le profil d'un client et ainsi déterminer son admissibilité à des prêts ou à d'autres services. Désormais, les États-nations font l'objet de formes comparables de surveillance et de profilage : les sociétés d'information publiques et privées recueillent de l'information qu'elles assemblent et font analyser par des humains ou des algorithmes en vue d'émettre des avis sur la situation des pays. Elles établissent ensuite le profil de ces pays pour évaluer leur solvabilité et leur rang sur le marché mondial. Comme pour les services bancaires aux consommateurs et les systèmes d'évaluation de la solvabilité, la majeure partie de l'infrastructure de surveillance économique mondiale relève des entreprises et elle n'est pas exploitée par les États ni par des organismes démocratiques internationaux. Les agences de notation qui évaluent la solvabilité des pays, telles que Standard & Poor's, Moody's et Fitch Ratings, sont des entreprises privées qui ne doivent rendre des comptes qu'à leurs actionnaires.

Mondialisation des normes

La troisième forme de mondialisation qui revêt de l'importance sur le plan de la surveillance est la normalisation. De plus en plus, des forums d'experts (comme ceux du G20 ou de l'OCDE) ou de spécialités techniques (comme le Frame Relay Forum, qui détermine les caractéristiques physiques des téléphones et d'autres connexions entre les périphériques de communication) s'emploient à établir des normes mondiales relatives à la sécurité et à la surveillance. Dans le passé, ces organisations adoptaient des normes qui n'avaient trait qu'aux technologies. Il ne faut pas négliger ces normes puisque, en tant que telles, elles ont une influence sur la facilité – ou la difficulté – avec laquelle les États peuvent surveiller les systèmes de communication. Néanmoins, depuis l'adoption de la norme sur la sécurité sociétale par l'Organisation mondiale de normalisation (ISO)[4], les normes dites « techniques » ne se limitent plus aux caractéristiques des caméras, par exemple, mais portent de plus en plus sur les pratiques, comme les procédures d'évacuation ou de surveillance.

Le moteur de cette normalisation est un amalgame d'intérêts gouvernementaux et commerciaux. La majorité des pays techniquement avancés ont adopté des lois (ou ont présenté des projets de loi) selon lesquelles les fournisseurs d'accès Internet doivent transférer le trafic de données personnelles

ou le contenu aux policiers et bloquer l'accès Internet aux utilisateurs qui contreviennent à la réglementation sur le droit d'auteur et les licences. Citons comme exemple l'Institut européen des normes de télécommunication, dont le champ d'action mondial signifie que les normes régissant l'interception légitime des communications peuvent être appliquées partout dans le monde. Ici la mondialisation des droits de propriété intellectuelle rencontre la mondialisation des communications et de l'informatique, ce à quoi les États ont réagi en favorisant un flux régulier du contenu commercial. Autrement dit, la surveillance effectuée par l'État renforce la sécurité et la concurrence entre les entreprises et ne tient pas nécessairement compte des intérêts des personnes ou des groupes.

Mondialisation des technologies

Enfin, de nombreux aspects de la mondialisation de la surveillance se présentent par des moyens plus subtils et hermétiques. Prenons par exemple la vidéosurveillance, qui s'est répandue partout dans le monde par l'intermédiaire du transfert de politiques publiques entre les nations et, surtout, par l'échange de « leçons apprises » entre le secteur privé (fabricants de technologies et agences privées de sécurité), les corps de police et les administrations locales, en plus de ceux que certains qualifient de « technocrates ambulants »[5]. De son côté, le transfert de politiques publiques repose sur des rapports officiels, des conférences internationales, la formation et l'échange de pratiques exemplaires (*best practices*) au moyen de publications spécialisées. Nombre des formes concrètes de surveillance que l'on peut voir de plus en plus fréquemment, en particulier dans les « villes du monde » connectées à l'échelle planétaire (Toronto, Montréal, Calgary et Vancouver) découlent de processus semi-officiels de partage du savoir, de commercialisation et d'apprentissage en matière de politique.

L'expansion de la surveillance est par conséquent presque isolée de l'évaluation que peuvent faire les universitaires ou les tiers de son efficacité. La recherche au Royaume-Uni a démontré clairement que les caméras de surveillance n'atteignaient pas leur objectif de lutte contre la criminalité[6], ce qui n'a pas empêché la montée en flèche de leur utilisation, ou d'autres pays de suivre l'exemple du Royaume-Uni. Les caméras de surveillance sont devenues de nos jours l'outil par excellence des professionnels de la gestion urbaine et du maintien de l'ordre, si bien que leur échec est souvent perçu comme un simple problème de mise en œuvre ou de technologie insuffisante, et jamais

comme un problème qui pourrait être inhérent à la technologie en tant que telle[7]. Dans le monde fermé des militaires, des policiers et des entreprises de technologie de sécurité, où les éléments se renforcent mutuellement, les profits et l'influence découlent trop souvent de la promotion de technologies de surveillance, peu importe ce que disent les universitaires et les militants au sujet de leur efficacité ou de leurs coûts sociaux.

La mondialisation de la surveillance en pratique

Dans la section suivante, nous nous pencherons sur quatre grands phénomènes mondiaux qui ont touché et continueront de toucher les Canadiens au XXIe siècle : contrôle frontalier, les enjeux connexes de la migration et des sans-papiers, le déplacement des manifestations de très grande envergure comme les Jeux olympiques et le recours accru aux véhicules aériens sans pilote (communément appelés drones).

La transformation des frontières canadiennes

Nombre des découvertes récentes présentées précédemment découlent de préoccupations au sujet de la mobilité croissante des personnes, des biens et de l'information. La mondialisation est synonyme d'une circulation plus large et plus rapide qu'auparavant des matières premières et des produits. Il en va de même pour les personnes, qu'elles fassent partie de l'élite des voyageurs d'affaires et des dignitaires, des touristes ou des masses d'immigrants à la recherche d'une meilleure vie ou tentant de fuir la guerre, une catastrophe ou la pauvreté. Or, ce flot de personnes et de biens s'est accompagné de menaces à la sécurité, de risques de transmission de maladies et de problèmes économiques, culturels ainsi que politiques. L'information, quant à elle, circule plus abondamment et plus rapidement que les biens matériels ou les personnes, y compris l'information sur ces biens et ces personnes. Bien que l'information fasse en permanence l'objet d'un tri, il existe des carrefours où les personnes, les biens et l'information se croisent ; les frontières en sont un.

La frontière canadienne, comme toutes les frontières d'ailleurs, se transforme. Des pressions s'exercent simultanément à l'échelle locale ainsi qu'à l'échelle mondiale pour l'ouverture de ces frontières pour des raisons économiques (faciliter la circulation des personnes et des biens) et pour la fermeture de celles-ci pour des raisons de sécurité (pour réglementer

les personnes et les cargaisons qui pourraient présenter un risque). Au Canada, deux grands organismes s'occupent des frontières. Le principal est l'Agence des services frontaliers du Canada (ASFC) qui est responsable de la sécurité des frontières. Constituée en 2003, l'ASFC administre maintenant 119 postes frontaliers terrestres et 13 aéroports internationaux. Le deuxième en importance est l'Administration canadienne de la sûreté du transport aérien (ACSTA). Créée en 2002, l'Administration est responsable du contrôle préalable à l'embarquement (les passagers et leurs effets personnels), de la vérification des bagages, du contrôle des non-passagers et de l'exécution du programme de cartes d'identité de zones réglementées dans 89 aéroports, tant au pays qu'à l'étranger.

D'autres organismes publics, tels que Citoyenneté et Immigration Canada (CIC), la GRC et le SCRS, coopèrent avec l'ASFC et l'ACSTA pour assurer la sécurité frontalière. Par ailleurs, dans le Grand Nord, ce sont les militaires canadiens qui s'occupent des patrouilles en région éloignée. Il est d'ailleurs probable que le Nord prenne de plus en plus d'importance dans le cadre de la surveillance des frontières. En effet, alors que les changements climatiques feront fondre la calotte glacière, de nouvelles routes maritimes s'ouvriront et l'exploration minière sera possible, de sorte que plusieurs pays pourraient revendiquer le même territoire. Cependant, la surveillance dans le Nord est complexe et entraîne des coûts faramineux. En 2008, le gouvernement canadien a présenté un projet impliquant l'usage de drones pour remplir cette mission, le Système interarmées d'acquisition d'objectif au moyen de véhicules aériens télépilotés de surveillance (JUSTAS). Toutefois, les coûts envisagés de cette initiative ne font qu'augmenter plus on la projette dans l'avenir. À la fin de 2012, on estimait que les coûts du projet s'élèveraient à un milliard de dollars et qu'il ne pourrait être mené à bien avant 2017[8].

La frontière canadienne est essentiellement un poste de triage pour un ensemble complexe de flux de personnes, d'information et de marchandises. Or, la plupart des procédures pour déterminer les individus et les biens qui sont acceptés et qui ne sont pas acceptés ne se déroulent pas à la frontière, mais plutôt ailleurs et avant l'arrivée. De nouvelles normes de portée mondiale sont actuellement élaborées pour le suivi et la vérification des biens et des personnes. À titre d'exemple, on appose une puce d'identification par radiofréquence sur les conteneurs d'expédition afin d'en surveiller étroitement les déplacements. Une puce doit également être installée sur certaines cargaisons, notamment la plupart des cargaisons d'animaux vivants ainsi que de carcasses d'animaux. Bien qu'on n'installe pas de puce sur les humains,

ils doivent utiliser un passeport lisible à la machine contenant une puce d'identification par radiofréquence et des identifiants biométriques de base (empreintes digitales et image faciale) selon la norme mondiale. De plus, le dossier passager et l'information préalable sur les voyageurs font l'objet d'un partage à grande échelle de part et d'autre des frontières[9].

Néanmoins, un tel échange transfrontalier peut entraîner des problèmes, car les autres pays pourraient ne pas appliquer les mêmes dispositions sur la protection de la vie privée et des données personnelles ou même sur l'application régulière de la loi que le Canada. Au cours des dernières années, le Canada a conclu plusieurs ententes et a adopté plusieurs programmes de sécurité frontalière. Il a par le fait même accru ses échanges de données avec les États-Unis et l'Union européenne. Le cadre principal de protection des renseignements personnels de l'Union européenne, que l'on appelle la Directive générale, est hautement compatible avec la législation canadienne sur la protection des renseignements personnels. La Directive a été adoptée en 1981 puis modifiée en 1995 et est devenue une norme mondiale puisqu'elle était le premier cadre législatif pour la protection des données personnelles[10]. À l'opposé, les États-Unis ne sont dotés d'aucune mesure de protection des renseignements personnels ; ils ont plutôt promulgué des lois pour certains secteurs, notamment pour les services bancaires et de la santé, et ont adopté des énoncés généraux dans les lois sur la protection de la vie privée. De plus, aucun cadre législatif fédéral ne régit les données personnelles recueillies à la frontière aux États-Unis. Pour compliquer encore davantage les choses, Washington a décidé en 2007 que son programme de surveillance des passagers – Secure Flight, couramment appelé « liste d'interdiction de vol » – ne serait pas assujetti aux dispositions déjà restreintes du *Privacy Act*.

L'influence qu'exercent les États-Unis sur le Canada se traduit déjà dans les mécanismes de partage des données et les accords extraordinaires conclus entre les deux pays. Au titre de ces accords et de ces mécanismes, les gardes-frontières et les policiers étatsuniens peuvent mener des activités en territoire canadien, notamment dans les aéroports internationaux où les passagers entrent dans ce qui est réputé territoire étatsunien dès avoir passé les douanes étatsuniennes, à l'intérieur des aéroports canadiens. Toutefois, le Canada a fait preuve d'une ambivalence pour d'autres aspects de la surveillance frontalière des États-Unis. À titre d'exemple, les agences frontalières canadiennes n'ont suivi qu'en partie l'exemple des États-Unis pour le recours aux scanneurs corporels. Or, selon les données disponibles, la technologie à balayage

corporel la plus répandue dans les aéroports américains, soit le scanneur à rétrodiffusion de rayons X produirait des images qu'il serait difficile de brouiller (ce qui est nécessaire pour protéger la vie privée) et aurait des risques pour la santé. Par conséquent, en 2013, la Transportation Security Administration a commencé à retirer les scanneurs à rayons X des aéroports aux États-Unis[11]. Par opposition, dans les aéroports canadiens, on utilise un scanneur à ondes millimétriques, lequel ne pose pas les mêmes risques pour la santé. De plus, Transports Canada tente d'appliquer des lignes directrices strictes de protection des renseignements personnels à leur utilisation[12]. Par ailleurs, le Canada a décidé de rendre le processus de balayage volontaire.

Les enjeux liés à la frontière canadienne incluent généralement les États-Unis, pour des raisons qui dépassent le simple fait que les deux pays se partagent la plus longue frontière terrestre du monde. En effet, l'influence stratégique des États-Unis, leur revendication de l'espace aérien et leur présence militaire se sont renforcées depuis le 11 septembre. Au cours de cette période, les priorités en matière de sécurité se sont raccordées à la libéralisation économique. Depuis l'entrée en vigueur de l'Accord de libre-échange nord-américain (ALENA) en 1994, la libéralisation économique a progressé au point où l'évolution logique des contrôles frontaliers est, selon certains, le « périmètre de sécurité nord-américain »[13]. Autrement dit, Ottawa adopterait les règlements des États-Unis pour les interactions aux frontières canadiennes et, en retour, Washington allégerait les restrictions qui rendent l'entrée des personnes et des biens si difficile.

Au début de 2011, le premier ministre, Stephen Harper, et le président des États-Unis, Barack Obama, ont signé une déclaration officielle intitulée « Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique. » Dans cette déclaration, les deux pays s'engageaient à « travailler de concert pour établir et valider l'identité des voyageurs, et mener des vérifications à la première occasion possible » et à « élaborer des normes techniques communes pour la collecte, la transmission et le rapprochement des données biométriques, afin de permettre la mise en commun, l'échange de l'information sur les voyageurs en temps réel ». Ces engagements signifient que des données personnelles confidentielles seront transmises instantanément d'un pays à l'autre. De plus, les deux pays prévoient « élaborer un système intégré d'entrée-sortie, qui comprend l'échange d'information pertinente pour l'entrée aux postes frontaliers terrestres, afin qu'une entrée documentée dans un pays permette de vérifier la sortie de l'autre pays »[14].



Qui dit obtention d'un passeport canadien, dit processus complexe de surveillance et d'identification (Source : © iStockphoto.com/AndrewWilliam)

Immigrants sans papiers

La hausse de l'immigration est l'une des facettes les plus importantes du monde interconnecté d'aujourd'hui. La Division de la population des Nations Unies estime que près de 214 millions de personnes ont migré d'un pays à un autre en 2010[15]. Le Canada est un pays qui repose sur l'immigration. À l'exception des peuples des Premières Nations, tous les habitants du Canada sont des descendants de l'immigration ou sont eux-mêmes des immigrants. Par ailleurs, beaucoup d'immigrants, dont plusieurs ont marqué l'histoire canadienne, sont arrivés sans détenir de document ou en ayant des antécédents juridiques douteux.

Pour les immigrants, la logique du contrôle frontalier et de la surveillance commence bien avant l'arrivée à la frontière à proprement parler ; ils tentent d'obtenir des documents valides et des documents d'identité pour pouvoir entrer dans les pays ciblés, comme le Canada. L'identification est devenue un commerce mondial important et constitue souvent l'infrastructure de la

surveillance que ce soit aux frontières ou à l'intérieur du pays. Cependant, bien que le Canada ait besoin d'immigrants pour son économie, nombre d'entre eux ne sont pas en mesure d'obtenir les documents nécessaires. Le régime de l'immigration au Canada a été renforcé, de sorte que les processus sont plus coûteux en temps et en argent et que certaines catégories d'immigrants sont exclues, en particulier les non-qualifiés et les moins instruits.

Ces mesures ont entraîné une hausse du nombre d'immigrants qui n'ont pas de documents d'identification ou les autorisations maintenant requises par le Canada pour entrer au pays. Les estimations du nombre d'immigrants sans papiers au Canada sont peu fiables : leur nombre oscillerait entre 35 000 et 500 000. Comme ils ne possèdent pas les documents d'identification, les visas ou les autres documents qui leur permettraient de naviguer dans le labyrinthe de plus en plus complexe de la surveillance administrative, les immigrants sans papiers sont victimes de trois types d'inégalité : droits inégaux, risques inégaux et temps de traitement inégal[16]. Ils n'ont accès ni aux soins médicaux, ni à l'aide sociale et ni aux mesures de protection de base qui semblent acquises pour les Canadiens. Ces gens sont sélectionnés pour des interrogatoires et des fouilles et se voient refuser l'entrée au pays sur la base souvent d'un préjudice, d'une erreur d'identification ou d'hypothèses non fondées[17]. Toutefois, le Canada n'est pas le seul à connaître ces difficultés. En effet, dans l'Union européenne, les immigrants doivent composer avec une hausse de la criminalité, des dispositions législatives contraignantes sur l'immigration et un climat grandissant de peur. On se préoccupe particulièrement du sort réservé aux enfants des immigrants sans papiers ; dans certains pays, ils seraient fréquemment emprisonnés[18]. Les services de police, en particulier la GRC et l'ASFC, ciblent les immigrants sans papiers et les soumettent à une surveillance plus approfondie au nom de la lutte contre la traite de personnes. Par contre, nombre de ces immigrants sont des cibles involontaires de cette surveillance, simplement parce qu'ils sont restés après la date d'expiration de leur visa ou parce qu'ils sont arrivés au Canada avec un permis de travail restreint à un seul employeur pour se retrouver avec un employeur abusif ou réticent à offrir le salaire minimum et les conditions d'emploi promises. Ces individus qui tentent de vivre leur vie sous le radar de la surveillance de l'État constituent une main-d'œuvre bon marché, vulnérable et marginale que les entreprises canadiennes embauchent pour exécuter des tâches ingrates.

La situation des immigrants nous révèle que, bien que les normes d'identification et de passeport soient de plus en plus uniformes, il n'existe aucun

régime international qui régit la mobilité transfrontalière des personnes[19]. Les dispositions actuelles tendent à se limiter aux conventions visant les travailleurs qualifiés. Même dans les cas où il existe un cadre de gouvernance unique, comme pour les réfugiés dont le droit d'asile est garanti par les Nations Unies[20], la situation n'est pas plus rose. La Division de la population des Nations Unies estime qu'il y avait près de 16,5 millions de réfugiés dans le monde entier en 2010[21]. La plupart seraient de simples réfugiés temporaires provenant d'États voisins. Il s'agit là d'un problème de surveillance puisque l'autorisation officielle pour qu'une personne traverse la frontière repose sur l'information personnelle contenue dans les documents d'identification ou dans les bases de données connexes. La façon dont cette information est recueillie et interprétée a des conséquences directes sur les personnes qui attendent la réponse à leur demande pour entrer au pays.

Les Canadiens sont fiers d'être reconnus comme une nation qui offre l'asile à ceux qui souhaitent échapper à la persécution, qu'il s'agisse d'esclaves fuyant les États-Unis, de sikhs du Panjab ou de réfugiés de la mer en provenance du Vietnam. Or, les récentes réformes des lois canadiennes ont emprunté une direction opposée, une direction moins accueillante. Conformément aux derniers changements, on qualifie maintenant l'arrivée des personnes qui demandent l'asile « d'arrivée irrégulière » et on a établi une liste des pays qui sont considérés comme sûrs (27 pays y figuraient en 2013) ; les demandes d'asile provenant de ces pays ne seront en règle générale pas examinées[22]. Parmi ces pays d'origine désignés, figure la Hongrie, ce qui signifie que les Roms de Hongrie ne peuvent demander l'asile au Canada même s'ils doivent faire face à un degré de persécution qui rend leur vie difficile dans ce pays. Nombre de ces personnes qui appartiennent à ces peuples nomades et qui autrefois demandaient l'asile au Canada pourraient aujourd'hui être dénoncées et considérées comme de faux revendicateurs ou des criminels[23].

Les villes canadiennes et les mégaévénements

Les grandes villes canadiennes rivalisent avec la concurrence à l'échelle mondiale pour les ressources et le prestige[24]. D'ailleurs, l'une des meilleures indications du statut mondial d'une ville est sa capacité à attirer des manifestations de très grande envergure. Parmi ces mégaévénements, mentionnons d'importantes compétitions sportives comme les Jeux olympiques ou la Coupe du Monde de la FIFA, des conférences politiques internationales

comme les sommets du G20, du G8 et des Nations Unies, et des festivals et des expositions culturels et commerciaux de premier plan comme les Expositions universelles. Lorsque des incidents comme l'explosion d'une bombe au marathon de Boston en avril 2013 se produisent et que les images prises par les caméras de surveillance de rue servent à confirmer l'identité des coupables, il n'est pas étonnant que l'expansion de la surveillance soit perçue comme un moyen de renforcer la sécurité.

Certes, les mégaévénements ne sont pas tous similaires. Il existe en effet une différence de dynamique entre les manifestations où un public (payeur) est invité, comme c'est le cas des Jeux olympiques, et celles qui sont interdites aux non-participants comme les sommets du G20. Ces événements présentent tout de même beaucoup d'éléments communs, entre autres le recours à des formes exceptionnelles de sécurité et de surveillance qui viennent temporairement compléter ou remplacer les lois nationales et locales ou encore qui vont à leur encontre[25]. Prenons l'exemple tristement célèbre des tribunaux sud-africains mis en place en 2010 pour la Coupe du Monde de la FIFA ; les autorités responsables du football ont littéralement pris le contrôle d'un aspect du régime juridique. Elles ont poursuivi en justice des amateurs et d'autres individus pour de nouveaux actes criminels contre la Coupe du monde de la FIFA. Il s'agissait essentiellement de crimes liés à la violation des droits exclusifs de commercialisation conférés aux commanditaires, comme le port de vêtements affichant la marque d'entreprises rivales[26]. Ces mesures exceptionnelles font souvent partie des exigences pour la tenue de tels événements et sont de plus en plus la norme dans les villes, et ce, peu importe les pratiques et les coutumes locales ou nationales. À titre d'exemple, le Comité International Olympique inclut maintenant la sécurité parmi les éléments essentiels dans le cadre de son processus officiel d'évaluation et transmet les pratiques exemplaires des anciennes villes-hôtes aux futures villes-hôtes[27] ; il s'agit là d'un bon exemple du processus mondial de « leçons retenues » dont nous avons parlé précédemment.

Par conséquent, les mesures de surveillance déployées dans les villes qui accueillent ces événements en viennent à se ressembler de plus en plus. Prenons par exemple la ville de Vancouver qui a accueilli les Jeux olympiques d'hiver en 2010 et la ville de Toronto qui a ensuite accueilli le sommet du G20 : dans les deux cas, on a observé une surveillance policière intensive des militants politiques que bon nombre ont trouvé intimidante et qui était conçue pour prévenir à la fois les actes criminels *et* les manifestations légitimes[28]. Les policiers ont également eu recours à des systèmes de vidéosurveillance

et ont partagé dans les médias sociaux des photos prises au moyen d'appareils photo et de caméras vidéo portatives pour identifier les manifestants[29].

Par ailleurs, ces mégaévénements servent fréquemment de banc d'essai pour de nouvelles technologies de surveillance et souvent les technologies utilisées demeurent en place même après l'événement. Dans le cas de Vancouver, les Jeux olympiques d'hiver ont manifestement servi de prétexte pour installer un système de vidéosurveillance qui n'aurait pas été politiquement acceptable dans des circonstances normales. Quant à Toronto, après le sommet du G20, seules quelques caméras de surveillance ont été laissées au centre-ville, mais les policiers ont conservé les autres caméras au cas où elles seraient utiles dans l'avenir[30]. Par ailleurs, les mégaévénements à l'étranger ont également servi à faire d'autres expérimentations. Des robots « renifleurs » ont servi à détecter les narcotiques lors de la Coupe du Monde de la FIFA tenue en Allemagne en 2006 et des dirigeables de surveillance volant à haute altitude ont été utilisés lors des Jeux panaméricains tenus à Rio de Janeiro en 2007[31]. De plus petits appareils aériens téléguidés ont été utilisés lors du championnat européen de l'Union des associations européennes de football en Suisse et en Autriche en 2008 et des systèmes d'accès biométriques ont été installés lors des Jeux olympiques de Londres en 2012[32]. Il devient de plus en plus normal de redéployer ces technologies lors d'événements ultérieurs.

Nombre des villes-hôtes d'événements d'envergure ont temporairement restructuré leurs rues en vue de renforcer la sécurité et la surveillance. La stratégie du périmètre de sécurité, par exemple, consiste à isoler le site de l'événement à l'intérieur de la ville et est inspirée de celle du « Cercle d'acier » utilisée par les autorités britanniques pour lutter contre le terrorisme à Belfast et à Londres[33]. Cette pratique est maintenant commune lors des réunions de l'envergure du G20 et des mégacompétitions sportives. De plus, ces événements nécessitent de plus en plus la modification de la circulation urbaine ainsi que la mise en place de « zones des partisans » qui isolent les spectateurs dans une zone clôturée et surveillée par caméras et qui permet de contrôler un public potentiellement turbulent. Enfin, parallèlement, ces zones sont souvent conçues pour soumettre les partisans à un amalgame de marketing intense et de surveillance à des fins commerciales[34].

La surveillance mobile et les drones

Les aéronefs téléguidés sont une autre forme de surveillance mondiale qui va croissant. Mieux connus sous le nom de « drones », ces appareils sans

pilote étaient à la base appelés véhicule téléguidé (VTG ; en anglais, *unmanned aerial* (ou *air*) *vehicles*, *UAV*). Selon un rapport produit récemment par le Government Accountability Office aux États-Unis, plus de 50 pays s'emploieraient à mettre au point 900 systèmes aériens sans pilote et 76 pays utiliseraient actuellement des drones[35]. De ce nombre, seuls trois pays, les États-Unis, le Royaume-Uni et Israël, utilisent des drones armés ; ces appareils servent donc pour la plupart strictement à la surveillance. Qui plus est, le marché des drones serait le secteur affichant la plus forte croissance de l'industrie mondiale de l'aérospatiale ; la valeur de ce marché se chiffrerait actuellement à 6,6 milliards de dollars des États-Unis par année et on s'attend à ce qu'elle double et atteigne 11,4 milliards de dollars au cours des dix prochaines années[36].

Les militaires, plus particulièrement l'armée des États-Unis, interviennent pour une bonne partie de cette croissance. La force aérienne étatsunienne patrouille maintenant la frontière Canada-ÉUA au moyen de drones Predator, les mêmes qu'elle a utilisés au Pakistan. Comme il a été mentionné précédemment, le gouvernement du Canada n'a toujours pas réussi quant à lui à se procurer des drones pour patrouiller la frontière dans le Grand Nord. Par ailleurs, les drones auraient de plus en plus d'application dans les marchés civils. De nouvelles associations de l'industrie qui ont beaucoup d'influence plaident pour une utilisation intérieure nationale et une utilisation commerciale privée des drones. À l'étranger, l'Association for Unmanned Vehicle Systems International fait campagne au nom des fabricants de drones. Au Canada, un groupe affilié à cette association, Systèmes télécommandés Canada, a été créé en 2010 à la suite de la fusion de deux plus petits groupes. Ces associations industrielles militent pour que la réglementation se limite à ce qu'ils estiment être strictement nécessaire.

Certaines unités des Forces canadiennes et des services de police, comme la GRC en Colombie-Britannique et en Saskatchewan ainsi que la Police provinciale de l'Ontario, se servent aussi de drones[37]. Ils les utilisent pour la surveillance côtière[38], de même que pour obtenir des images des accidents de la route et pour effectuer d'autres tâches de vérification et de surveillance pour l'application de la loi. Les drones servent également à plusieurs autres activités publiques outre le maintien de l'ordre. Prenons par exemple le secteur de l'immobilier, qui les utilise pour enregistrer des vidéos spectaculaires à peu de frais des grandes propriétés à des fins publicitaires (cet usage s'est accru substantiellement) et les organismes non gouvernementaux qui s'en servent pour surveiller la détérioration de l'environnement



Les drones sont de plus en plus utilisés pour des applications civiles. (Source : © iStockphoto.com/alexsalcedo)

causée par l'industrie[39]. Enfin, les forestières en fiducie, les chercheurs environnementaux et les sociétés privées ont également recours aux drones pour inspecter et évaluer des territoires qui ne sont pas accessibles par d'autres moyens[40].

Il existe également des différences importantes entre les drones utilisés à l'intérieur du pays et la plupart de ceux qui sont utilisés par les militaires. Ces derniers sont à peu près de la même taille qu'un aéronef piloté conventionnel et peuvent fonctionner sur de longues distances et pendant de longues périodes. Quant aux drones utilisés à l'intérieur du pays, on les appelle souvent des microvéhicules aériens sans pilote ; ils ont tendance à être petits et légers (certains sont si compacts qu'ils peuvent être transportés dans un sac à dos). De plus, ils sont faciles d'utilisation et, dans bien des cas, ressemblent aux avions téléguidés à assembler à la maison. Par conséquent, leurs usages individuels et collectifs risquent d'augmenter[41]. D'ailleurs, selon l'industrie, le seul obstacle à la croissance des marchés civils pour les drones serait la réglementation aérienne nationale[42]. Or, les citoyens, les groupes de

défense des droits civils et les organes de réglementation privés ont tous de bonnes raisons d'être préoccupés par la croissance de la surveillance intérieure humaine au moyen de drones. Le service de recherches du Congrès américain a publié récemment un rapport dans lequel il soulignait ces préoccupations[43]. De plus, lors d'une allocution devant le Congrès, l'Electronic Privacy Information Center a affirmé que pour utiliser des UAV, les policiers devraient avoir un mandat et que les opérateurs de drones devraient être assujettis à des restrictions quant à l'utilisation des données et à des obligations de transparence. Par ailleurs, les Canadiens ont eux aussi besoin de précisions quant aux usages commerciaux, personnels et policiers de ces appareils. Heureusement, les médias populaires en Amérique du Nord commencent à soulever ces questions ; d'ailleurs, l'auteur d'un article paru récemment dans *The Atlantic* se demandait justement : « Si mon véhicule aérien sans pilote survole la maison de mon voisin, s'agit-il d'une intrusion ? »[44]

Certes, la taille réduite des drones a rendu la surveillance plus facile à transporter et plus dissimulée. Néanmoins, un domaine de recherche et de développement clé pour les appareils de surveillance mobile est la technologie biomimétique, qui imite des animaux ou des plantes. On tente le plus fréquemment d'imiter des oiseaux, des serpents ou des insectes avec ces dispositifs. D'ailleurs, AeroVironment, principal fabricant de drones aux États-Unis et plus important fournisseur d'hélicoptères policiers téléguidés, a récemment produit un robot fonctionnel partiellement télécommandé par radio et partiellement autonome, le « Nano Hummingbird » (nanocolibri)[45]. Ces percées nous montrent que la surveillance optique risque de devenir encore plus secrète, mais ne verra pas sa puissance s'affaiblir.

Conclusion

Pour comprendre les tendances de la surveillance au Canada, il importe de les placer dans le contexte non seulement national, mais également international des lois, des normes, des pratiques, des technologies et des organismes. La mondialisation contribue à accélérer le développement de la surveillance dans tous les domaines, surtout dans la nouvelle économie mondiale. De plus, cette surveillance touche les simples consommateurs et les voyageurs dans les transactions qu'ils effectuent quotidiennement ainsi que dans d'autres sphères de la sécurité. Les nouveaux accords mondiaux, internationaux ou bilatéraux énoncent fréquemment des engagements officiels pour la

prise de nouvelles mesures de surveillance, comme les listes d'interdiction de vol, l'information préalable sur les voyageurs et les accords frontaliers. La mondialisation crée également un marché de plus en plus concurrentiel et novateur pour toutes les technologies de surveillance, des plateformes militaires les plus coûteuses aux appareils personnels bon marché, en passant par les drones. Par ailleurs, ces technologies sont de plus en plus hybrides et les dispositifs commercialisés ne présentent que de légères variantes entre les usages militaires et les usages civils. La diffusion des normes mondiales – que ce soit par la norme ISO sur la « sécurité sociétale » ou par l'échange informel de pratiques exemplaires qui ne font aucune distinction entre les différents contextes et antécédents – peut faire en sorte que des intérêts exclusifs en matière de sécurité semblent neutres et peut contribuer à désamorcer le débat sous le prétexte que l'on ne fait qu'appliquer des pratiques qui semblent déjà acceptées à l'échelle mondiale.

Notes

1 Rebecca Anna Stoil, « Israel, Canada Sign Security Accord », *Jerusalem Post,* 29 novembre 2007, http://www.jpost.com/Israel/Israel-Canada-sign-security-accord.

2 Voir Andrew Stevens, « Surveillance Policies, Practices and Technologies in Israel and the Occupied Palestinian Territories: Assessing the Security State », *Nouvelle transparence : surveillance et tri social, document de travail 4*, novembre 2011, http://www.sscqueens.org/sites/default/files/2011-11-Stevens-WPIV_0.pdf.

3 Philip Rosen, *Le Centre de la sécurité des télécommunications ; l'organisme de renseignement le plus secret du Canada* (Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, BP343-F, 1993) http://www.parl.gc.ca/Content/LOP/researchpublications/bp343-f.htm.

4 Organisation mondiale de normalisation, *Sécurité sociétale – Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle*, ISO/PAS 22399:2007, http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50295.

5 Wendy Larner et Nina Laurie. « Travelling Technocrats, Embodied Knowledges: Globalising Privatisation in Telecoms and Water », *Geoforum* 41, nº 2 (2010), p. 218-226.

6 Voir, par exemple, Martin Gill et Angela Spriggs, *Assessing the Impact of CCTV,* étude du Home Office Research 292 (Londres, Home Office Research, Development and Statistics Directorate, 2005), https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf.

7 Pour une analyse des pratiques et de la logique des politiques canadiennes, voir Sean P. Hier, *Panoptic Dreams: Streetscape Video Surveillance in Canada* (Vancouver, University of British Columbia Press, 2010).

8 David Pugliese, « Canada's Drone Squadron Still Stalled, with Neither Planes nor Troops », *Ottawa Citizen*, 27 décembre 2012.

9 Une fois de plus, les États-Unis sont à l'origine des passeports contenant une étiquette d'identification par radiofréquence et d'identifiants biométriques, initialement par l'intermédiaire du sommet du G8 tenu à Sea Island, en Géorgie, le 10 juin 2004. Voir Statewatch,

« G8 Meeting at Sea Island in Georgia, USA, Sets New Security Objectives for Travel », 2004, http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm.

10 Union européenne, Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *Journal officiel* n° L 281, 23 novembre 1995, p. 0031-0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML.

11 Mike M. Ahlers, « TSA Removing 'Virtual Strip Search' Body Scanners », *CNN*, 18 janvier 2013, http://www.cnn.com/2013/01/18/travel/tsa-body-scanners/index.html.

12 Canada, Ministère des Transports, *Scanners corporels aux principaux aéroports canadiens*, 2013, http://www.tc.gc.ca/fra/medias/documents-scanners-corporels-7131.html.

13 Pour une analyse critique, voir Dana Gabriel, « The Integration of Canada into a U.S. Dominated North American Security Perimeter, » *Global Research,* 18 juin 2013, http://www.globalresearch.ca/the-integration-of-canada-into-a-u-s-dominated-north-american-security-perimeter/5339525.

14 Canada, Premier ministre, *Par-delà la frontière : une vision commune de la sécurité et de la compétitivité économique à l'intérieur du périmètre,* déclaration du premier ministre du Canada et du président des États-Unis d'Amérique, Washington (D.C.), 2011, http://pm.gc.ca/fra/nouvelles/2011/02/04/dela-la-frontiere-vision-commune-de-la-securite-et-de-la-competitivite.

15 Nations Unies, Division de la population, *International Migrant Stock: The 2008 Revision*, Nations Unies, 2009, http://esa.un.org/migration/.

16 Robert Pallitro et Josiah Heyman, « Theorizing Cross-border Mobility: Surveillance, Security and Identity », *Surveillance and Society* 5, n° 3 (2008), p. 315-333.

17 Pour des exemples et des faits vécus, se reporter à la Coalition pour la surveillance internationale des libertés civiles, *Contrôles frontaliers et listes de surveillance*, 2010, http://surveillancedesvoyageurs.ca.

18 Plate-forme pour la Coopération Internationale sur les Sans-papiers, *Droits fondamentaux des sans-papiers en Europe : principaux sujets de préoccupation de PICUM en 2010*, Bruxelles, 2010, http://picum.org/picum.org/uploads/publication/Annual%20Concerns%202010%20FR.pdf.

19 Programme des Nations Unies pour le développement, *Lever les barrières : Mobilité et développement humains,* Rapport sur le développement humain de 2009, http://hdr.undp.org/en/media/HDR_2009_FR_Complete.pdf, p. 43.

20 Pour en savoir plus sur le droit d'asile garanti, se reporter au Haut Commissariat des Nations Unies pour les réfugiés, *Convention relative au statut des réfugiés* de 1951 et *Protocole relatif au statut des réfugiés* de 1967, http://www.unhcr.fr/4b14f4a62.html.

21 Nations Unies, Division de la population, *International Migrant Stock: The 2008 Revision*, Nations Unies, 2009, http://esa.un.org/migration/.

22 Nicholas Keung, « Changes to Refugee System: Immigration Minister Jason Kenney Lays Out Criteria for 'Safe' Countries », *Toronto Star,* 30 novembre 2012, http://www.thestar.com/news/canada/article/1296161--changes-to-refugee-system-immigration-minister-jason-kenney-lays-out-criteria-for-safe-countries.

23 Cynthia Levine-Rasky, « Who Are You Calling Bogus? », *Canadian Dimension* 46, n° 5 (2012), p. 12-14.

24 Voir Peter J. Taylor, *World City Network: A Global Urban Analysis* (Londres et New York, Routledge, 2003).

25 Voir, par exemple, Alessandra Renzi et Greg Elmer, *Infrastructure Critical: Sacrifice at Toronto's G8/G20 Summit* (Winnipeg, Arbeiter Ring, 2012).

26 Marina Hyde, « World Cup 2010: Fans, Robbers and a Marketing Stunt Face Justice, Fifa Style », *The Guardian*, Royaume-Uni, 20 juin 2010, http://www.guardian.co.uk/football/2010/jun/20/world-cup-2010-fans-marketing-justice-fifa.

27 Philip Boyle, « Knowledge Networks: Mega-events and Security Expertise », dans Colin J. Bennett et Kevin D. Haggerty (dir.), *Security Games: Surveillance and Control at Mega-events* (Londres et New York, Routledge, 2011), p. 184-199.

28 Jeffrey Monaghan et Kevin Walby, « Making Up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression », *Policing and Society* 22, nº 2 (2012), p. 133-151.

29 Daniel Trottier, « Policing Social Media », *Canadian Review of Sociology/Revue canadienne de sociologie* 49, nº 4 (2012), p. 411-425.

30 « Toronto Police Want to Keep Most G20 Security Cameras », *CTV News,* 15 novembre 2010, http://toronto.ctvnews.ca/toronto-police-want-to-keep-most-g20-security-cameras-1.575057.

31 Francisco R. Klauser, « Spatial Articulations of Surveillance at the FIFA World Cup 2006TM in Germany », dans Katja Franko Aas, Helene Oppen Gundhus et Heidi Mork Lomell (dir.), *Technologies of InSecurity: The Surveillance of Everyday Life* (Abingdon, Royaume-Uni, et New York, Routledge-Cavendish, 2009) p. 61-80 ; et David Murakami Wood, « Cameras in Context: A Comparison of the Place of Video Surveillance in Japan and Brazil », dans Aaron Doyle, Randy Lippert et David Lyon (dir.), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Londres et New York, Routledge, 2012) p. 83-99.

32 Francisco R. Klauser, « Commonalities and Specificities in Mega-Event Securitization: The Example of Euro 2008 in Austria and Switzerland », dans Colin J. Bennett et Kevin D. Haggerty (dir.), *Security Games: Surveillance and Sport Mega-Events* (Londres et New York, Routledge, 2011), p. 120-136 ; et Pete Fussey et Jon Coaffee, « Balancing Local and Global Security Leitmotifs: Counter-Terrorism and the Spectacle of Sporting Mega-Events », *International Review for the Sociology of Sport* 47, nº 3 (2012), p. 268-285.

33 Jon Coaffee, David Murakami Wood et Peter Rogers, *The Everyday Resilience of the City* (Basingstoke, Royaume-Uni, Palgrave Macmillan, 2009).

34 David Murakami Wood et Kirstie Ball, « Brandscapes of Control? Surveillance, Marketing and the Co-construction of Subjectivity and Space in Neo-liberal Capitalism », *Marketing Theory* 13, nº 1 (2013), p. 47-67.

35 États-Unis, Government Accountability Office, *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports,* GAO-12-536, juillet 2012, http://www.gao.gov/assets/600/593131.pdf, p. 13, 9.

36 Teal Group, « Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast », 11 avril 2012, http://tealgroup.co/index.php/about-teal-group-corporation/press-releases/66-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast.

37 Voir Alexandra Gibb, « Privacy Concerns Hover over RCMP Drones in British Columbia », *TheThunderBird.ca,* 29 mars 2012, http://thethunderbird.ca/2012/03/29/privacy-concerns-hover-over-rcmp-drones-in-british-columbia/ ; et Sigrid Forberg, « Une initiative qui prend de l'altitude ; Un nouvel outil facilite les enquêtes », *La Gazette de la GRC* 74, nº 1 (2012), http://www.rcmp-grc.gc.ca/gazette/vol74n1/trends-dernierestendances-fra.htm.

38 Sur la surveillance côtière, voir Colin Kenny, « Pourquoi le Canada a besoin de drones », *National Post,* Sénateur Collin Kenny, 28 février 2012, http://colinkenny.ca/fr/p102659/.

39 Pour le premier, voir Neal Ungerleider, « Unmanned Drones Go from Afghanistan to Hollywood », *Fast Company*, 15 février 2012, http://www.fastcompany.com/1816578/unmanned-

drones-go-afghanistan-hollywood ; et pour le seconde, voir Alexandra Gibb, « A Drone Field Guide », Conseil international du Canada, *Opencanada.org*, 31 mai 2012, http://www.opencanada.org/features/the-think-tank/a-drone-field-guide/.

40 Julia Horton, « Attack of the Drones to Fight Tree Rot in Scotland », *The Scotsman*, 28 octobre 2012, http://www.scotsman.com/news/environment/attack-of-the-drones-to-fight-tree-rot-in-scotland-1-2602637.

41 Voir « Drones Work the Skies for Police, Scientists, Media », *CBC News*, 22 mars 2012, http://www.cbc.ca/news/technology/story/2012/03/22/technology-thecurrent-civilian-drones.html.

42 Steve Zaloga et David Rockwell, « UAV Market Set for 10 Years of Growth », *Earth Imaging Journal*, 2011, http://eijournal.com/uncategorized/uav-market-set-for-10-years.

43 « EPIC to Congress: Protect Privacy Against Drone Surveillance », 5 novembre 2012, http://epic.org/2012/11/epic-to-congress-protect-priva.html. Voir aussi Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, service de recherches du Congrés américain, 3 avril 2013, http://www.fas.org/sgp/crs/natsec/R42701.pdf ; et *Electronic Privacy Information Center, Testimony and Statement for the Record of Amie Stepanovich, Association Litigation Counsel, Electronic Privacy Information Center, Field Forum on the Impact of Domestic Use of Drone Technology on Privacy and Constitutional Rights of All Americans*, 25 octobre 2012 (Rice University, Houston), http://epic.org/privacy/drones/EPIC-Drones-Testimony-102512.pdf.

44 Alexis C. Madrigal, « If I Fly a UAV over My Neighbor's House, Is It Trespassing? », *The Atlantic*, 10 octobre 2012, http://www.theatlantic.com/technology/archive/2012/10/if-i-fly-a-uav-over-my-neighbors-house-is-it-trespassing/263431/.

45 AeroVironment. « Nano Humingbird », 2013, http://www.avinc.com/nano ; Kevin D. Haggerty et Daniel Trottier, « Surveillance and/of Nature: Monitoring Beyond the Human », *Society and Animals* (2013), doi: 10.1163/15685306-12341304.



Intégration de la surveillance dans la vie de tous les jours

De la surveillance des personnes à la surveillance des objets

Dans l'extrait « Une journée dans la vie de Farah » présenté dans la première tendance, peu des nombreuses occurrences de surveillance visant Farah et sa famille peuvent être associées sans hésiter à de la surveillance si une personne ne sait pas comment les renseignements personnels sont recueillis et traités en coulisse. La majorité de la surveillance est intégrée dans notre quotidien de façon harmonieuse. Elle s'insère même de manière presque imperceptible dans les accessoires et les situations que nous considérons maintenant comme essentiels à la vie moderne.

L'évolution vers une surveillance omniprésente est facilitée en partie par l'intégration de capteurs, d'identifiants et de caméras dans des objets courants et dans l'environnement construit. Ce qui autrefois était fait à des endroits précis ou au moyen de dispositifs particuliers est maintenant devenu une caractéristique des véhicules, des rues, des maisons et des milieux de travail que nous utilisons tous les jours. Nous utilisons le téléphone cellulaire pour communiquer avec notre famille et nos amis et ce, sans nous arrêter au fait que, du coup, nous laissons savoir à la compagnie de téléphone où nous nous trouvons en tout temps. Nous regardons les photos de nous sur Facebook sans être freinés par le fait que Facebook est maintenant le principal développeur de logiciel de reconnaissance faciale dans le monde. En effet, ses algorithmes peuvent nous identifier dans des photos même si nous

La rue dans la mire des citoyens : surveiller la vidéosurveillance

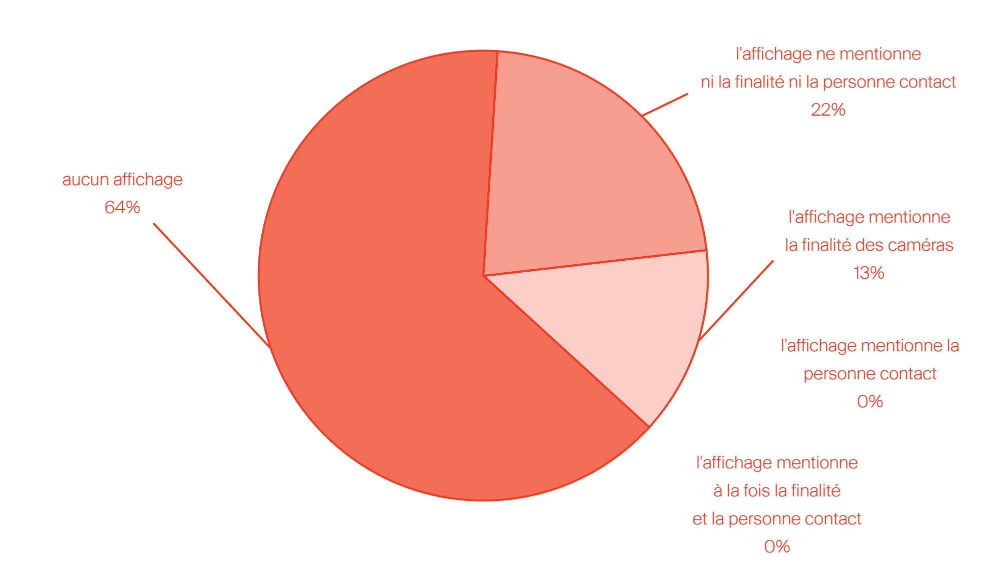
On sait bien peu de choses sur l'utilisation de la vidéosurveillance par le secteur privé au Canada. Bien que les caméras de surveillance soient essentiellement installées à des fins commerciales, la majorité de la recherche effectuée jusqu'à maintenant portait sur des usages gouvernementaux[1]. Des faits élémentaires comme le nombre approximatif de caméras exploitées par le secteur privé n'ont pas encore été établis. On en sait peu sur les pratiques et les politiques du secteur privé quant au traitement de l'information vidéo personnelle capturée par les caméras.

Une étude menée récemment et financée par le Commissariat à la protection de la vie privée a tenté de combler certaines de ces lacunes[2]. Des chercheurs de l'Université de Toronto se sont rendus dans plus de 300 établissements commerciaux de la région du Grand Toronto et ont observé la présence de caméras de surveillance dans près de la moitié de ces entreprises. Ils ont noté plus particulièrement que les quatre plus grandes sociétés dans chacun des secteurs suivants : services bancaires, vente de vêtements, restauration rapide ainsi qu'électronique et grands magasins faisaient toutes de la vidéosurveillance. Le grand magasin Sears du Centre Eaton de Toronto à lui seul en avait 90. Près de 60 % des installations n'étaient assorties d'aucune affiche qui indiquaient aux clients la présence de caméras et de ces affiches aucune – pas même une seule – ne répondait aux exigences minimales prévues dans les lignes directrices établies conjointement par les commissaires à la protection de la vie privée du Canada, de l'Alberta et de la Colombie-Britannique[3]. Les affiches requises ne sont pas coûteuses et, pour la vidéosurveillance effectuée dans le secteur public, ces exigences sont dans la majorité des cas satisfaites. Une affiche visible et intelligible sur laquelle on peut lire le nom du propriétaire, le but de la collecte de données et le nom d'un responsable au sein de l'organisme à qui adresser les demandes de renseignements suffit.

Après avoir consigné la présence de caméras et des affiches, les chercheurs de l'Université de Toronto ont demandé au gérant de plusieurs établissements des renseignements au sujet des pratiques organisationnelles de protection de la vie privée puis lui ont remis une formule de demande d'accès à des renseignements personnels pour lui demander une copie de l'enregistrement vidéo de leur visite. Légalement, le gardien des renseignements personnels est tenu de répondre dans les 30 jours et de fournir au demandeur un accès à ses renseignements. Les résultats obtenus sont tristes, mais en disent long. Malgré un suivi systématique et déterminé de 45 entreprises après la première demande, seules trois ont fourni les images vidéo demandées. Dans les 100 autres cas où aucun suivi n'a été fait après la demande initiale, les résultats sont encore pires.

L'absence d'affiches et le peu de réponses obtenues à la suite des demandes d'accès aux renseignements personnels montrent que le non-respect de la *Loi sur la protection des*

Caractéristiques de l’affichage



Exigences d’affichage (Source : gracieuseté d’Andrew Clement, Université de Toronto)

renseignements personnels et les documents électroniques (la loi qui réglemente la protection de la vie privée dans le secteur privé) est répandu. Si les opérateurs des caméras, qui sont l’icône de la surveillance, enfreignent la loi de façon flagrante et en toute impunité, cela ne présage rien de bon pour les Canadiens. La vidéosurveillance continue de prendre de l’expansion grâce aux possibilités de stockage numérique moins coûteuses, à la transmission en réseau et à l’analyse automatisée des images. De plus, elle s’intègre de plus en plus à notre environnement physique commun ainsi qu’à nos attentes culturelles. Les risques continueront donc de croître à moins que des formes novatrices et efficaces de contrôle public soient mises au point.

1. « Introduction », *Eyes Everywhere: The Global Growth of Camera Surveillance*, publié sous la direction de Aaron Doyle, Randy Lippert et David Lyon (Londres et New York, Routledge, 2012), p. 17.
2. Andrew Clement, Joseph Ferenbok, Roxanna Dehghan, Laura Kaminker, Simeon Kanev, et Silvia Valdman, *Un détective privé « intelligent » dans les lieux publics? L’analyse par vidéosurveillance, les nouvelles menaces à la vie privée et les solutions de rechange pour la protection des renseignements personnels*, rapport final, 23 juillet 2011, présenté au Commissariat à la protection de la vie privée du Canada, http://www.priv.gc.ca/resource/cp/2010-2011/p_201011_01_f.asp.
3. Canada, Commissariat à la protection de la vie privée, Commissaire à l’information et à la protection de la vie privée de l’Alberta et Commissaire à l’information et à la protection de la vie privée de la Colombie-Britannique, *Lignes directrices sur la surveillance vidéo au moyen d’appareils non dissimulés dans le secteur privé*, mars 2008, http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_f.pdf.

n'y sommes pas étiquetés. Enfin, les appareils photo numériques peuvent intégrer l'heure, la date et les coordonnées GPS sur toutes les photos prises.

L'intégration de capacités de surveillance dans des dispositifs communs et des environnements courants est une tendance qui dure depuis longtemps. Elle est étroitement liée à l'augmentation générale de la surveillance, de même qu'à l'expansion plus récente de la surveillance mobile et géodépendante ; nous avons abordé ces deux sujets précédemment. Le rythme soutenu des changements technologiques dans le réseau numérique et les technologies qui y sont associées sont le moteur le plus évident du processus d'intégration. Non seulement le nombre d'appareils ayant des fonctions de sonde, d'enregistrement, de transmission et de traitement augmente, mais individuellement ces appareils sont également de moins en moins onéreux et de plus en plus petits. Cela contraste fortement avec l'augmentation du nombre de voitures au début du XXe siècle ; à ce moment, les voitures, les routes et certains aspects de l'infrastructure de soutien sont devenus extrêmement visibles dans des situations de tous les jours. Or, l'expansion du réseau numérique se produit à une plus grande échelle et encore plus rapidement, mais elle se fait essentiellement hors de la vue. Bien que nous puissions voir des gens utiliser leur téléphone intelligent, leur ordinateur portable et d'autres appareils, ces dispositions ne constituent que la pointe d'un gigantesque iceberg ; le plus gros de l'iceberg est le matériel qui est caché derrière des murs ou sous terre et les activités bourdonnantes qui se répandent pratiquement partout au moyen des ondes radioélectriques[1].

Au fur et à mesure que nous avons adopté ces technologies, nous avons intégré la surveillance dans notre conception des « acquis » du monde dans lequel nous vivons. On parle maintenant de la surveillance comme d'un élément normal de l'éducation des enfants, du travail et des voyages. De plus, nombre d'entre nous observons régulièrement les autres et acceptons d'être observés au quotidien, et ce, sans y réfléchir à deux fois. Une telle intégration nous empêche de repérer, de comprendre, de débattre et de réglementer de façon démocratique les pratiques de surveillance qui se sont imbriquées dans le quotidien de la vie moderne.

Pour nous aider à visualiser et à comprendre la surveillance autour de nous et pour faciliter la discussion, il est utile de faire une distinction entre deux approches d'intégration de la surveillance : dans la première, la surveillance sert principalement à mettre au point de nouveaux moyens de recueillir des renseignements personnels ; et dans la seconde, les capacités de surveillance sont présentées comme un *ajout* à une activité existante ;

cette approche dépend des renseignements personnels qui sont amassés comme une partie inhérente de l'activité initiale ou qui sont générés simplement comme un sous-produit. Les caméras de vidéosurveillance sont un exemple de la première situation qui est une forme de surveillance plus facilement repérable, tandis que l'utilisation d'un enregistreur de frappe dans les ordinateurs d'un bureau ou l'interception des communications dans l'infrastructure d'Internet sont des exemples du dernier. La surveillance présentée comme un « ajout » est plus répandue et plus difficile à cerner. Nous exposerons dans les prochains paragraphes que dans les deux cas, l'intégration de la surveillance la rend plus difficile à détecter, de sorte qu'il est difficile d'obliger les responsables à rendre des comptes.

La surveillance comme point de mire : surveillance à usage déterminé

L'exemple le plus frappant de l'intégration discrète, dans notre vie quotidienne, d'appareils conçus spécialement pour la surveillance, est la croissance extraordinaire des divers types de caméras de surveillance. La majeure partie de cette croissance prend la forme de caméras de surveillance installées dans les rues et les centres commerciaux pour renforcer la sécurité. D'ailleurs, la caméra est probablement le symbole le mieux connu de la surveillance.

Bien que le Royaume-Uni soit reconnu depuis longtemps comme le chef de file en ce qui concerne l'implantation de caméras de surveillance, le Canada lui a en quelque sorte emboîté le pas en faisant de cette forme de surveillance une caractéristique omniprésente de la vie urbaine moderne[2]. Les caméras de surveillance sont notamment de plus en plus utilisées le long des routes pour repérer les conducteurs qui font des excès de vitesse ou qui passent sur un feu rouge. Les voitures de taxi dans les grandes villes sont également munies de caméras afin de prendre une image de chaque passager. Dans ces cas, les images enregistrées sont normalement examinées seulement s'il y a des preuves qu'il y a eu une infraction ou un incident.

Même si ces caméras sont le signe le plus visible de la surveillance, les gens ne sont en général pas conscients de leur présence[3], en partie parce que ces caméras sont relativement petites et banales et qu'elles sont souvent installées discrètement au plafond ou sur de hauts murs extérieurs hors de notre champ de vision. Peu d'opérateurs de caméras de surveillance tenteront d'attirer l'attention sur leur installation. Même si les entreprises sont

tenues par la loi canadienne d'afficher des avis indiquant aux gens la présence de caméras de surveillance, une étude réalisée en 2011 a révélé que seul un tiers des installations commerciales sondées étaient accompagnées d'un tel avis et que, lorsqu'un tel avis est affiché, il était conçu et placé de façon à ne pas être remarqué[4]. De plus, les avis en tant que tels n'étaient systématiquement pas conformes aux exigences minimales énoncées dans la loi canadienne sur la protection des renseignements personnels.

Une application de surveillance visuelle très poussée et délicate sur le plan de la protection de la vie privée est la lecture automatisée des plaques d'immatriculation. Cette application est d'ailleurs de plus en plus utilisée dans les parcs de stationnement et sur les routes. Les systèmes de lecture automatisée des plaques d'immatriculation reposent sur des techniques de reconnaissance optique de caractères qui permettent de capturer les numéros d'immatriculation. Les données ainsi recueillies sont comparées à une liste des plaques associées à des voitures recherchées par la police ou sont stockées dans une base de données en vue d'une utilisation ultérieure. Ces dispositifs sont également installés sur des structures surplombant les autoroutes et servent à percevoir les péages, signaler les suspects ou suivre les déplacements de personnes suspectées. Les policiers les utilisent aussi dans leur voiture pour rechercher automatiquement les véhicules qui figurent dans leur liste de surveillance. Ils peuvent ainsi distribuer une contravention ou intercepter les conducteurs sur-le-champ.

La surveillance en tant qu'ajout : surveillance des transactions

Les entreprises et les organismes gouvernementaux ont rapidement commencé à incorporer des dispositifs de surveillance particuliers dans l'environnement construit. Cependant, les capacités de surveillance qui ont été ajoutées à des appareils et des transactions qui avaient été conçus à l'origine pour d'autres usages sont beaucoup moins visibles et ont une portée, une intensité et des conséquences beaucoup plus importantes. Dans les années 1960, on a commencé à avoir de plus en plus recours aux ordinateurs pour la tenue de dossiers et le traitement des transactions, de sorte que les possibilités d'intégrer la surveillance à un vaste éventail d'environnements ont été décuplées. Au départ, cette surveillance était incorporée au milieu de travail, dans les grands bureaux, et ciblait surtout le travail courant et les employés de rang inférieur. Ensuite, les directeurs ont commencé à faire

usage des données de production informatisées ; ce sous-produit qui était généré rapidement par les systèmes en place pouvait inclure le total des saisies au clavier, le temps de réponse, le volume des ventes et la production. Il servait à gérer le rendement des employés, processus que Zuboff a appelé « informating », la collecte d'information visant la gestion et l'automatisation du travail[5]. Souvent, cette surveillance prenait la forme d'un suivi du rendement individuel par rapport à des cibles préétablies ; les employés étaient ensuite récompensés ou punis selon le cas. À l'époque, les mécanismes plus approfondis de surveillance ont soulevé la controverse, en particulier dans les milieux syndiqués et ont même suscité une enquête du gouvernement fédéral au début des années 1980[6].

L'automatisation des processus administratifs a ouvert la voie au traitement électronique des transactions et à la surveillance de clientèle. Si autrefois ces transactions étaient complétées sur des appareils fixes, à usage déterminé et appartenant à des entreprises (comme un guichet automatique ou un terminal de point de vente), au cours des dix dernières années elles ont migré vers les appareils mobiles, polyvalents et appartenant à des individus (téléphones intelligents par-dessus tout). Par le fait même, on a commencé à intégrer des capacités de surveillance à ces appareils personnels. Prenons par exemple le scandale d'écoute téléphonique de *News of the World* au Royaume-Uni, qui a éclaté lorsqu'on a appris que des journalistes avaient intercepté les messages vocaux de milliers d'individus. Cet exemple montre tout le potentiel de surveillance des transactions au moyen des réseaux de télécommunications desquels les appareils mobiles dépendent[7]. Pour une analyse plus approfondie de ces techniques de surveillance, se reporter à la Tendance 5.

Perfectionnement des cartes d'identité aux fins de surveillance

Examinons un autre exemple qui montre comment la surveillance a été intégrée en catimini à des articles communs et à caractère très personnel : les améliorations numériques apportées récemment à nos documents d'identification. Les documents d'identification sont un élément essentiel à la vie moderne. En effet, nous devons présenter des documents d'identification dans un nombre sans cesse croissant d'endroits : lorsque nous magasinons, lorsque nous entrons dans un immeuble ou d'autres locaux, lorsque nous utilisons le transport en commun, lorsque nous traversons la frontière, et

L'omniprésence de la surveillance intégrée : le système HospitalWatch*Live* d'Infonaut

La surveillance à but médical est sans doute l'une des formes de surveillance que nous tolérons le plus facilement. Par exemple, il importe de faire un suivi étroit des maladies infectieuses pour diagnostiquer les personnes qui pourraient en être atteintes ainsi que pour protéger la population d'une épidémie dévastatrice. Infonaut, une entreprise canadienne de technologie médicale qui se spécialise dans le contrôle des infections en se fondant sur des données probantes, est un chef de file mondial pour ce qui est de repousser les limites de la surveillance médicale approfondie. Infonaut a démarré après que 41 Torontois sont morts du syndrome respiratoire aigu sévère (SRAS) au début de 2003[1]. L'un des premiers produits de l'entreprise a été le système Infection Watch Live, une application cartographique de surveillance et d'alerte pour les cas de maladies gastro-intestinales et de maladies respiratoires qui s'appuie sur des flux d'information en temps réel.

Infonaut met actuellement à l'essai son système HospitalWatch*Live*, qui vise à lutter contre la propagation des maladies infectieuses dans les hôpitaux par le suivi en temps réel de l'emplacement et des déplacements des patients et du matériel. Des étiquettes transpondeurs à ultrasons fabriquées par Sonitor sont apposées sur les patients, le personnel, les lits, les chariots, les distributeurs de savon et de gel, les commodes et l'équipement médical qui est près des sites possibles de contamination ou de transmission des infections. La position des étiquettes est consignée toutes les deux ou trente secondes par un réseau de microphones à ultrasons installé sur les murs et au plafond des corridors et dans les chambres et salles de toilettes des patients. Les flux de données ainsi créés permettent de faire un suivi précis des gens et des objets, de leurs proximités relatives et, par inférence, le parcours des pathogènes. On peut lire sur le matériel de l'entreprise :

Le déploiement du Système de localisation en temps réel en milieu clinique permet aux hôpitaux de suivre et de consigner tous les déplacements, tous les contacts et toutes les interactions entre les patients, le personnel et le matériel. On obtient ainsi un dépistage instantané des contacts basé sur le risque qui permet de faire une analyse prévisionnelle de la structure des infections et des réservoirs pathogènes[2].

Infonaut a conçu son système pour qu'il offre les avantages suivants :

Le respect de l'hygiène des mains : pour promouvoir le respect des normes de nettoyage des mains auprès des cliniciens ou pour faire le suivi des contacts entre le clinicien et le patient.

Le dépistage automatisé des contacts : pour faire le suivi des risques d'infection par les multiples degrés de séparation.

La sécurité au travail : pour protéger le personnel au moyen d'alertes immédiates au sujet de ceux qui pourraient avoir été en contact avec une personne qui aurait été exposée à une maladie infectieuse.



P-Tag de Sonitor® pour les patients et le personnel (Source : technologies de Sonitor, http://www.sonitor.com/technology/tags/p-tag)

Détection des foyers d'infection : pour prévenir la transmission continuelle à partir des réservoirs pathogènes possibles.

Infonaut admet que cette forme de surveillance approfondie peut porter hautement atteinte à la vie privée et que l'efficacité du système dépend de la volonté de coopérer des différents intervenants. Par conséquent, l'entreprise a essayé d'intégrer la protection de la vie privée dans le mode de fonctionnement du système. Elle s'est efforcée de donner le plus d'information possible aux médecins, aux infirmières et au personnel de nettoyage de première ligne qui participent au projet pilote. Conformément à la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario, l'hôpital est le gardien des renseignements recueillis. Aussi, les rapports produits par le système semblent n'être utilisés que pour l'objectif de lutte contre les infections et non pour la prise de mesures disciplinaires. Les patients reçoivent des renseignements de base sur le système et sont soumis au même processus de consentement que celui appliqué pour les procédures médicales invasives. Environ 10 % des patients ont refusé d'utiliser le système[3]. Ce programme pilote montre qu'un suivi étroit des gens dans un cadre institutionnel est faisable sur le plan technique. Bien que le système semble se fonder sur une approche qui respecte le droit à la vie privée, il reste à voir si les mêmes précautions seront prises pour les renseignements personnels si la technologie HospitalWatch*Live* passe de l'état expérimental à un produit commercialisé et déployé dans des cadres différents.

1. Organisation mondiale de la santé, « Summary Table of SARS Cases by Country, 1 November 2002–7 August 2003 », http://www.who.int/entity/csr/sars/country/country2003_08_15.pdf.
2. Infonaut, « HospitalWatch*Live* », 2012, http://www.infonaut.ca/.
3. Communication personnelle du Docteur Colin Furness à l'intention du personnel d'Infonaut, 7 octobre 2012.

ainsi de suite. Les documents d'identité que nous utilisons le plus souvent sont des cartes de plastique typiques qui se rangent aisément à l'endroit désigné dans notre portefeuille ou notre sac à main. Nous sommes maintenant habitués de montrer ces cartes ou d'autres documents d'identification pour qu'un employé autorisé puisse faire une inspection visuelle rapide avant de nous donner l'autorisation.

L'intégration de capacités de surveillance aux cartes d'identité a connu une progression par étape. En effet, l'intégration a suivi le rythme du perfectionnement des technologies numériques. La première percée – et elle est sans doute la plus importante – est l'établissement d'un lien direct entre les documents d'identification et leur base de données correspondante. La lecture informatisée des données sur les cartes d'identité, en particulier de l'identifiant unique, permet une vérification en temps réel grâce à une base de données permettant de déterminer si le titulaire de la carte peut être autorisé. Conséquence de cette avancée, la fonction première d'une carte d'identité est passée de la certification que le détenteur a un statut particulier (conducteur autorisé, membre d'un groupe, citoyen) à la connexion entre la personne et son « double de données ». On entend par double de données la totalité de l'information personnelle numérique sur une personne. De plus, le balayage d'une carte ajoute la plupart du temps une nouvelle donnée au dossier de la personne. L'établissement d'une connexion entre la collecte de données, les données stockées et le processus d'autorisation automatisée permet une fine gestion des populations, c'est-à-dire un triage efficace et discret des personnes en vue de les classer dans des catégories de traitement définies par l'organisme[8].

Au cours des vingt dernières années, deux autres avancées technologiques numériques ont été intégrées aux cartes d'identité communes, comme les permis de conduire, les cartes santé et les passeports : la biométrie et la puce d'identification par radiofréquence (IRF). Ces changements ont eu peu d'incidence sur l'apparence extérieure des cartes, mais ont ouvert la porte à une augmentation du potentiel de surveillance. La plupart du temps, les étiquettes IRF et la biométrie se conjuguent à un nombre sans cesse croissant de bases de données et à des efforts discrets mais soutenus visant l'intégration des données et des processus de collecte. Ainsi, il devient étonnamment facile d'accumuler des renseignements personnels. Ces techniques permettent de lire les données des cartes dans un éventail large et varié de transactions. Elles promettent aux détenteurs des cartes des avantages tout en renforçant encore davantage le lien entre eux et leur double de données.

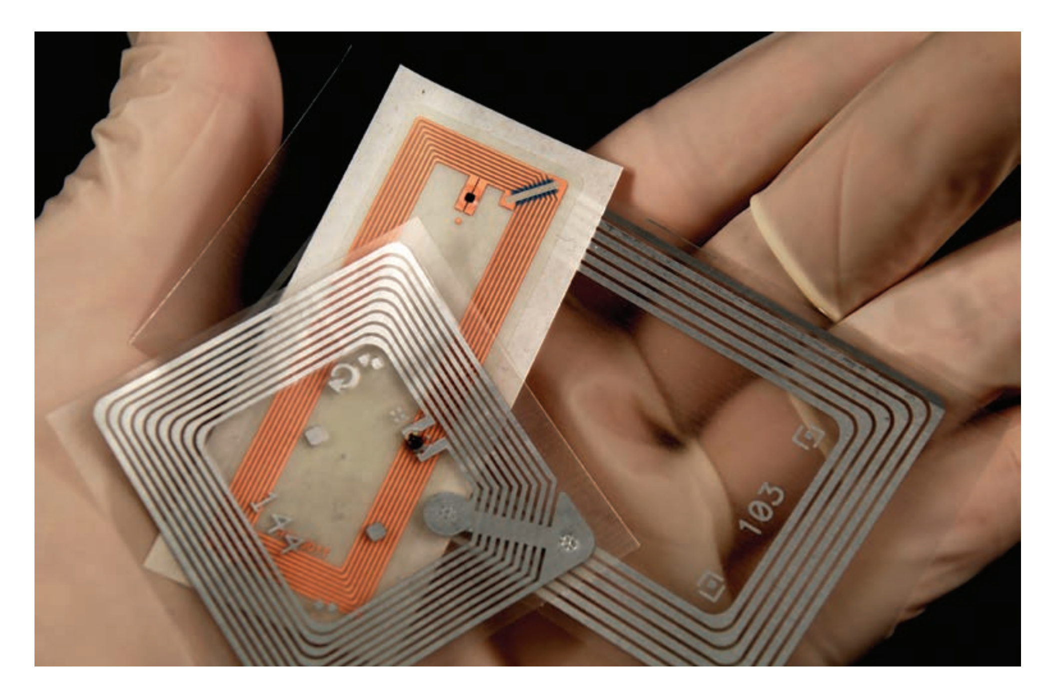
Le projet de carte intelligente de l'Ontario a été l'une des premières – et des plus ambitieuses – tentatives entreprises au Canada pour « améliorer » des cartes d'identité conventionnelles au moyen de technologies numériques. Proposé à la fin des années 1990 par Mike Harris, premier ministre du Parti conservateur à l'époque, le projet avait pour objectif de lancer une carte polyvalente permettant d'accéder à toute une série de services gouvernementaux. Grâce à des attributs biométriques les utilisateurs pourraient vérifier ou « authentifier » leur identité et confirmer qu'ils sont bien le titulaire de la carte. À cette fin ils auraient soumis leurs empreintes digitales, iris ou autre et le lecteur aurait comparé les images obtenues avec celles enregistrées. Comme pour bien d'autres initiatives de mise en place d'un système d'identification controversé et trop ambitieux, le projet s'est noyé dans l'incompréhension du public et ne put surmonter la difficulté technique de fusionner les nombreux services impliqués au sein d'un système unique. Bien que le gouvernement provincial ait subtilement mis de côté le projet qui battait de l'aile en 2002, les aspirations qui étaient au cœur de ce projet, soit l'établissement d'un registre de toute la population, la mise en œuvre de bases de données intégrées et l'authentification biométrique n'ont pas été étouffées et ont joué un rôle important dans d'autres initiatives d'identification lancées par la suite au Canada. Parmi celles-ci, citons la « BC Services Card », laquelle combine la carte santé et le permis de conduire en Colombie-Britannique et prend appui sur une base de données d'attributs faciaux biométriques communs.

Les mesures prises par l'administration Bush à la suite des attentats du 11 septembre 2001, bien qu'elles soient arrivées trop tard pour sauver le projet de carte intelligente en Ontario, ont constitué un levier spectaculaire et lucratif pour les industries de la gestion de l'identité et de sécurité dans l'ensemble. Les effets ont été ressentis presque immédiatement au Canada. Le Canada et les États-Unis se sont empressés de rédiger une Déclaration sur la frontière intelligente et un Plan d'action qu'ils présentèrent à la fin de cette année-là. Cette Déclaration prévoyait la mise en place d'une carte d'identité biométrique commune en Amérique du Nord et ce, même si ni son utilité sur le plan de la sécurité ni son efficacité sur le plan technique ne pouvaient être prouvées. Parallèlement, dans un cas manifeste de blanchiment politique[9], les États-Unis ont poussé l'Organisation de l'aviation civile internationale (OACI) à adopter un nouveau « passeport électronique » ; ce passeport devait comprendre une puce qui permettrait sur demande de transmettre une photographie numérique du visage permettant l'identification biométrique du titulaire du passeport. Ce mode de transmission ne nécessite aucun contact

et le passeport peut être balayé à distance sans que son titulaire le sache. Le Canada a appuyé ce changement de norme et a offert d'adopter le passeport électronique en 2005. Bien que le gouvernement fédéral ait reporté à maintes reprises le lancement public de ce passeport électronique, il a discrètement commencé à intégrer ces attributs biométriques essentiels aux passeports conventionnels qui ont été délivrés depuis[10]. D'ailleurs, Passeport Canada a déjà adopté des normes plus rigoureuses pour les photos (interdiction de sourire) afin de faciliter la reconnaissance faciale automatisée au moment de présenter la demande de passeport et pour une authentification ultérieure.

L'Initiative relative aux voyages dans l'hémisphère occidental est entrée en vigueur aux États-Unis le 1er juin 2009 et exige l'utilisation d'attributs biométriques. Comme ils appréhendaient que les nouvelles mesures de sécurité ralentissent le passage à la frontière, les gouvernements de plusieurs États et provinces situés le long de la frontière canado-américaine ont mis de l'avant le « permis de conduire amélioré » ou « plus » ; cette carte devait être une solution de rechange rapide, facile et économique au passeport[11]. Selon les exigences établies par le Department of Homeland Security (DHA) des États-Unis, une puce IRF a été intégrée au permis de conduire amélioré. En balayant la carte, les gardes-frontières ont accès à une image numérique du visage du conducteur et à d'autres renseignements figurant dans son dossier. L'une des caractéristiques requises de la puce IRF est qu'elle doit permettre une distance de lecture relativement longue[12] ; initialement mise au point pour la gestion du bétail et de chaînes d'approvisionnement, elle est conçue pour être lue dans un rayon de dix mètres de l'antenne. Si l'on ajoute cette caractéristique à l'absence de cryptage ou d'autres formes de protection des renseignements personnels, le DHS n'aurait pu choisir une norme moins sûre et plus axée sur la facilitation de la surveillance. Les défenseurs des libertés civiles et des représentants de l'industrie de l'identification ont élevé des objections concernant l'atteinte possible à la vie privée, mais le DHS a fait la sourde oreille. Néanmoins, le seul aspect positif est que peu de Canadiens et d'Étatsuniens ont opté pour le permis de conduire amélioré, dont le nombre est bien inférieur aux prévisions. On ne sait toutefois pas si un jour il ne sera plus possible de l'éviter[13].

Bien que l'ampleur du projet visant à créer une carte d'identité biométrique commune pour l'Amérique du Nord ait été réduite, en raison de l'opposition soulevée et des difficultés de mise en œuvre, nombre des ingrédients qui composaient le projet sont déjà utilisés dans d'autres initiatives. À titre d'exemple, dans le cadre de l'Initiative REAL-ID[14] et malgré



Certaines puces d'intenfication à radiofréquence peuvent être lues à près de 10 mètres de distance et plusieurs ne permettent pas le chiffrement de leur contenu. Sécurité ou surveillance ? (Source: iStockphoto.com/albn)

une forte résistance, le gouvernement étatsunien a tenté de transformer *de facto* le permis de conduire délivré par les États en carte d'identité nationale. Au Canada, les gouvernements fédéral et provinciaux ont collaboré discrètement à la mise au point d'un système national de gestion de l'identité similaire, qui prendrait appui sur les documents d'identification existants[15].

En ce qui a trait à la surveillance, la préoccupation la plus grave concernant ces systèmes d'identification au Canada est peut-être que l'inscription routinière des Canadiens adultes à des systèmes biométriques a lieu sans susciter de débat public et avec de bien minces indications qu'un contrôle est bel et bien exercé. On y est parvenu essentiellement en capturant des photographies faciales à haute résolution pour les permis de conduire, les cartes santé et les passeports qui servent à la reconnaissance faciale automatisée. Ces capacités ont attiré l'attention du public dans la foulée des émeutes qui ont suivi la finale de la Coupe Stanley en juin 2011 à Vancouver. La Insurance Corporation of British Columbia avait alors offert au service de police de Vancouver l'accès à son logiciel de reconnaissance faciale et à sa base de

données d'images presque infaillible pour identifier les personnes soupçonnées d'actes criminels[16]. La police a toutefois choisi de mettre au point sa propre base de données et n'a pas demandé l'ordonnance d'un tribunal pour avoir accès à ces données.

Surveillance approfondie d'Internet

Un troisième enjeu relatif à l'intégration de la surveillance a commencé à poindre depuis 2000 : l'interception et l'inspection des données circulant sur Internet. Le principal aspect de la surveillance d'Internet qui a attiré l'attention du public et qui a suscité la controverse est la surveillance « en périphérie » d'Internet. Du point de vue des utilisateurs ou des clients d'Internet, la capture des données par les logiciels de surveillance intégrés aux navigateurs (fichiers de témoins et pixels invisibles) est critiquée depuis les années 1990[17]. Récemment, les mêmes critiques ont été ravivées par la présence de ces mêmes logiciels dans les appareils mobiles sans fil (applications de localisation sur les téléphones intelligents iPhone et Android). De la même façon, du côté des serveurs, il y a un débat permanent au sujet de l'accès secret, entre autres, aux courriels et aux publications sur les médias sociaux des plateformes appartenant à Google, Facebook, Microsoft et d'autres grands fournisseurs de service.

À la suite de l'explosion des services en ligne au cours des dix dernières années, plus particulièrement des applications de réseautage social, les gens partout sur la planète ont commencé à alimenter de leur plein gré, et parfois avec enthousiasme, les bases de données d'entreprises avec des quantités phénoménales de données souvent de nature très personnelle. L'accès à cette mine de données détaillées est un élément clé des modèles d'affaires appliqués par les entreprises concernées. En règle générale, celles-ci utilisent ces données à des fins publicitaires ou les vendent à des tiers qui en font un usage commercial. Ces pratiques présentent évidemment des risques d'atteinte à la vie privée. Par contre, les consommateurs se sont montrés jusqu'à maintenant enclins à accepter ce risque, soit parce qu'ils ne sont pas bien informés, soit parce qu'ils en tirent des avantages pratiques ou en échange de l'accès gratuit aux services offerts. Ces bases de données et les précieuses révélations qu'elles apportent sur les activités et les comportements d'une vaste portion de la population constituent un attrait de taille pour les organes gouvernementaux de sécurité et d'application de la loi.

Dans le cas du programme PRISM, mentionné à la Tendance 6, la National Security Agency (NSA) aux États-Unis s'est assuré un accès automatique aux bases de données de neuf grands fournisseurs d'accès Internet, contournant les règles qui ordonnent qu'on s'adresse à un tribunal pour avoir accès aux données d'un individu. Bien qu'ils soient puissants et prospères, les fournisseurs d'accès Internet n'ont pas pu s'opposer à la demande du gouvernement étatsunien et ont dû lui accorder un accès en bloc à leurs données. Ils ont même invoqué, tout comme la NSA elle-même, la trop vague exemption tiers dans le domaine de la protection des renseignements personnels pour justifier la légalité de cet accès[18]. En ce qui concerne les Canadiens et les habitants d'autres pays, l'accès conféré à la NSA n'est entravé par aucune restriction légale. Conformément aux ententes de partage des données de longue date, les organismes gouvernementaux canadiens ont accès aux données recueillies par la NSA.

L'intégration aux dispositifs des clients et des serveurs de capacités de surveillance en périphérie d'Internet suscite certes la controverse. Or, c'est dans les profondeurs de l'épine dorsale d'Internet que les formes les plus alarmantes de surveillance d'Internet sont secrètement intégrées. Les routeurs gigantesques, hébergés dans des tours de bureaux discrètes en plein centre des grandes villes, transfèrent des milliards de paquets de données chaque seconde entre les câbles à fibres optiques et les dirigent vers leur destination. Au cours des dix dernières années, les gouvernements et les entreprises ont installé du matériel qui intercepte, analyse, sélectionne et stocke les données qui passent par ces commutateurs cruciaux ou ces points d'interconnexion Internet. Un grand nombre et une gamme de plus en plus grande d'activités sont menés au moyen d'Internet ; il est donc stupéfiant de constater qu'il est possible de suivre furtivement toutes les communications personnelles de millions de personnes et à quel point cette surveillance présente de nombreuses ramifications.

L'analyse des volumes gigantesques de données passant dans Internet constitue un défi technique redoutable, surtout si l'on souhaite faire cette analyse suffisamment rapidement pour que les données puissent servir au maintien de l'ordre ou à la gestion. Néanmoins, bien que la rapidité et les capacités des routeurs aient augmenté, les modes d'interception et les raisons de le faire se sont également accrus. On entend par « inspection approfondie des paquets » (IAP ; en anglais, *deep packet inspection*) les techniques qui permettent aux transporteurs Internet de lire le contenu de nombreux messages et fichiers qui sont transmis par Internet[19]. Un paquet

de données est un élément d'information informatique structuré transmis sur Internet : il est composé d'un « en-tête » contenant les renseignements d'adressage et des « données utiles » renfermant le contenu du message. On peut faire une analogie entre ces paquets de données et une carte postale ou une lettre. D'une part, les défenseurs de la vie privée aiment mieux l'analogie de la lettre puisque malgré qu'ils admettent que l'en-tête doit pouvoir être lu par des intermédiaires, pour eux le contenu devrait rester confidentiel. D'autre part, les fournisseurs de service préfèrent l'analogie de la carte postale puisqu'ils estiment que le contenu doit être accessible à tous. Bien que le cryptage puisse protéger le contenu des regards indiscrets, l'en-tête (l'adresse du destinataire) ne doit pas être crypté pour que le paquet soit acheminé. Ordinairement, des mesures de protection des renseignements personnels moins rigoureuses sont appliquées aux renseignements de l'en-tête ainsi qu'à d'autres métadonnées de communication, telles que l'heure, l'emplacement et la durée. Toutefois, comme on peut maintenant recueillir et analyser automatiquement des masses de métadonnées, qui peuvent en dire très long, les défenseurs du droit à la vie privée soutiennent que des mesures de protection similaires à celles employées pour le contenu du message devraient s'y appliquer.

Au Canada, l'IAP a éclaté au grand jour lorsque les défenseurs de la vie privée ont fait part de leurs préoccupations quant aux pratiques des grands fournisseurs d'accès Internet, comme Bell et Rogers. En effet, on soupçonnait ces fournisseurs de ralentir ou d'accélérer délibérément les communications de certains utilisateurs ou de certaines applications, comme BitTorrent (www.bittorrent.com), service gratuit à la mode de partage de fichiers Internet de pair à pair. En 2009, ces fournisseurs ont indiqué au Conseil de la radiodiffusion et des télécommunications canadiennes, lors d'audiences sur les pratiques de gestion du trafic Internet[20], qu'ils doivent être autorisés à utiliser l'IAP afin d'établir l'ordre de priorité du trafic sur Internet. Par exemple, il faut que les applications qui dépendent d'une livraison à temps (par exemple, voix sur IP) enregistrent moins de retard que les applications qui en sont moins dépendantes (courriels et transfert de fichiers). Des recherches menées par la suite ont révélé qu'au moins une douzaine de grands fournisseurs d'accès Internet au Canada avaient installé du matériel servant à l'IAP[21]. Bien que Telus ait brièvement bloqué l'accès à un site Web à l'appui d'un syndicat en se basant sur les renseignements de l'en-tête[22], il n'y a jusqu'à maintenant aucune preuve directe que les fournisseurs canadiens utilisent l'IAP pour surveiller les utilisateurs ou bloquer l'accès à des sites légitimes.

Cependant, il n'en va pas de même pour le matériel vendu par les fabricants canadiens, tels que Netsweeper, aux régimes autoritaires du Moyen-Orient. Ces régimes ont recours à ces dispositifs pour localiser les groupes d'opposition et censurer les sites Web pour des motifs religieux ou politiques[23].

Pour ses branchements clandestins sans mandat, la National Security Agency (NSA) aux États-Unis a largement recours aux techniques d'IAP en vue de surveiller la population. En 2003 elle a commencé à installer du matériel de surveillance dans les principales stations pivot de routage Internet de grands fournisseurs américains comme AT&T et Verizon. Ces activités hautement secrètes ont été révélées avec fracas par Mark Klein, technicien d'AT&T en 2006. Peu après avoir pris sa retraite, Klein a divulgué que la NSA avait pris des dispositions pour qu'AT&T installe des diviseurs à fibres optiques et du matériel d'interception du trafic Internet dans son principal centre de communications au 611, rue Folsom, à San Francisco. Comme elle possède des installations similaires pour d'autres passerelles Internet aux quatre coins du pays, l'administration américaine espionne vraisemblablement la population tout entière. Comme aucun mandat n'avait été lancé pour ces interceptions, une quarantaine de cas impliquant les fournisseurs et le gouvernement ont été portés devant les tribunaux[24]. Or, ces litiges ont été paralysés par l'adoption par le Congrès de modifications à la *Foreign Intelligence Surveillance Act* de 2008[25]. Ces modifications visaient à élargir la portée de la surveillance permise par la loi et à conférer rétroactivement aux fournisseurs du secteur privé une immunité contre les poursuites. Le gouvernement fédéral étatsunien a bloqué systématiquement les procès intentés contre lui en affirmant que les demandeurs n'avaient pas la qualité pour agir puisque ces derniers ne pouvaient prouver qu'ils avaient été victimes d'une surveillance secrète ou en invoquant l'exemption relative aux secrets d'État[26].

Peu importe les protections juridiques qui s'appliquent aux citoyens étatsuniens, aucune protection du genre ne s'applique à ceux qui sont ciblés par les activités similaires d'interception des communications à l'étranger. La NSA appelle ces activités une collecte de données « en amont »[27]. Outre l'installation de diviseurs à fibres optiques dans les grands centres de communication (infrastructure), lorsque l'exploitant du centre ne coopère pas suffisamment, la NSA a adopté une technique plus audacieuse qui consiste à se brancher directement sur les câbles reliant les centrales. Comme la majorité du trafic Internet international est transmis au moyen de câbles à fibres optiques sous-marins, cette technique nécessite l'installation de branchements aux points d'atterrissage ou même au milieu de l'océan[28].



Boomerang canadien de Toronto à Toronto (Source : http://www.ixmaps.ca/index.php)

Outre les données auxquelles la NSA a accès en espionnant les communications Internet à l'échelle internationale, les Canadiens sont souvent visés par les interceptions faites sur le réseau Internet national par les États-Unis, et ce, même si eux-mêmes et le destinataire de leur communication se trouvent au Canada. En effet, près du tiers du trafic canadien est acheminé par les États-Unis, et ce routage se fait presque toujours par l'une des villes où l'on soupçonne fortement la NSA de mener des activités de surveillance (New York, Chicago, et Seattle)[29]. Ce routage à effet boomerang peut survenir même entre deux institutions publiques canadiennes situées dans la même ville au pays. À titre d'exemple, des paquets de données acheminés de l'Université de Toronto au Régime d'aide financière aux étudiantes et étudiants de l'Ontario situé à quelques rues du campus passent par New York et Chicago – deux villes où la NSA aurait installé des diviseurs – avant de revenir à Toronto. Comme l'information passe par les États-Unis, elle est assujettie aux dispositions du *Patriot Act* (2001), qui permet aux organismes gouvernementaux américains de jeter un coup d'œil à l'information transitant par les États-Unis, même si cette information est stockée à l'extérieur des États-Unis.

Même le trafic Internet qui est transmis par les fournisseurs de services de télécommunications canadiens et qui demeure intégralement à l'intérieur des frontières canadiennes pourrait faire l'objet d'une forme similaire de surveillance du réseau prescrite par l'État canadien. D'ailleurs, cette situation a attiré l'attention du public en 2012 lorsque le gouvernement conservateur a déposé de nouveau le projet de loi C-30 sur l'accès légal, renommé au dernier

moment *Loi sur la protection des enfants contre les cyberprédateurs*. Le projet de loi en tant que tel ne faisait pas référence aux cyberprédateurs, sauf dans son titre[30]. Toutefois, les principales dispositions de la loi qui visaient à élargir les pouvoirs des organes d'application de la loi incluaient notamment l'accès aux « données de l'abonné » lorsque ces organismes en font la demande aux fournisseurs Internet. Aucune autorisation juridique ni aucun motif raisonnable de soupçonner un acte criminel ne sont requis ; les fournisseurs sont tenus de fournir les données demandées. Le projet de loi investissait également les organismes d'application de la loi de nouveaux pouvoirs selon lesquels ils peuvent exiger aux fournisseurs de service de stocker des données sur un client et de produire ces données sur demande[31].

Par ailleurs, le projet de loi C-30 exigeait que les systèmes des fournisseurs de services de télécommunications soient conçus pour que les policiers puissent facilement intercepter le trafic Internet[32]. Comme la conformité à cette disposition engendrerait des coûts importants pour les transporteurs, le gouvernement a mené pendant plus d'un an de vastes consultations avant de déposer le projet de loi. Il a notamment consulté les plus importantes entreprises de télécommunications afin de déterminer qui devraient assumer ces coûts et s'il serait faisable de suivre les comportements des utilisateurs dans un environnement infonuagique de plus en plus complexe[33]. Ce long processus de négociation forme un vif contraste avec l'absence totale de consultation publique. Néanmoins, en réaction à la promesse électorale faite par les Conservateurs en 2011, selon laquelle ils allaient présenter de nouveau le projet de loi s'ils étaient réélus, des groupes de défense des libertés civiles et des droits Internet ont formé la Coalition Arrêtez l'espionnage en ligne[34]. Comme nous l'avons mentionné à la Tendance 3, la Coalition a lancé une campagne d'envoi de lettres et a produit diverses vidéos[35]. De plus, elle a mis en ligne une pétition que plus de 145 000 personnes ont signée pour demander au gouvernement de cesser d'espionner les citoyens sur Internet. Lorsque le projet de loi a finalement été déposé par le gouvernement le 14 février, il a provoqué une telle controverse publique qu'il a été renvoyé directement au Comité pour être modifié. Il fut ensuite discrètement abandonné un an plus tard[36]. Toutefois, la surveillance d'Internet que ce projet de loi devait autoriser est déjà une réalité et ce, en toute conformité avec les lois sur la protection des renseignements personnels en vigueur. Les dispositions législatives sur la protection des renseignements personnels régissant le secteur privé – la *Loi sur la protection des renseignements personnels et les documents électroniques* – permettent déjà, dans certaines circonstances,

aux fournisseurs de services de télécommunications de communiquer aux enquêteurs de police des renseignements personnels sans que les clients concernés le sachent ou y consentent et sans avoir besoin d'un mandat[37].

Cette situation témoigne de plusieurs éléments importants de l'état actuel de la surveillance Internet au Canada :

- Le gouvernement fédéral et les grandes entreprises privées *feront* de la surveillance d'une manière ou d'une autre, dans le secret et hors de tout contrôle ; ils continueront également de prôner des lois qui se répercuteront sur la relation fondamentale entre les citoyens et l'État.
- Les lois sur la protection des renseignements personnels en vigueur ne sont pas suffisamment rigoureuses et ne peuvent faire opposition à ces atteintes aux libertés civiles acquises.
- La surveillance est une préoccupation publique répandue, peu importe l'appartenance politique.
- Une opposition politique structurée peut former une résistance efficace contre une surveillance excessive d'Internet.

Conclusion

Les pratiques de surveillance mettent à rude épreuve la vie privée et d'autres libertés civiles. La tendance à l'intégration vient accentuer ces préoccupations, en particulier parce qu'elle rend la surveillance à la fois de moins en moins visible et de plus en plus banale. Comme ces pratiques sont rarement visibles de l'extérieur et sont habituellement groupées avec d'autres activités plus légitimes, il devient extrêmement difficile de garantir l'ouverture et la transparence nécessaire pour obliger les responsables de la surveillance à rendre démocratiquement des comptes. Selon les lois canadiennes sur la protection des renseignements personnels, les organismes responsables de cette surveillance ont pour responsabilité principale de rendre les pratiques accessibles au public. Or, comment savoir si elles sont rendues publiques ou non ? En règle générale, il faut qu'une infraction soit commise puis qu'une enquête approfondie soit réalisée pour que les utilisations abusives de la surveillance éclatent au grand jour. Enfin, par le temps qu'elles soient dénoncées, ces infractions sont devenues une pratique répandue dans l'industrie. Il devient alors très difficile de prendre des recours après coup.

Notes

1 Voir Andrew Blum, *Tubes: Journey to the Center of the Internet* (New York, Harper Collins, 2013).

2 Voir *Eyes Everywhere: The Global Growth of Camera Surveillance,* publié sous la direction de Aaron Doyle, Randy Lippert et David Lyon (Londres et New York, Routledge, 2012) ; Emily Jackson, « Hundreds of Unnamed Cameras Watching Vancouver », *TheThunderBird.ca,* 10 décembre 2009, http://thethunderbird.ca/2009/12/10/hundreds-of-unnamed-cameras-watching-vancouver/ ; Andrew Clement, Joseph Ferenbok, Roxanna Dehghan, Laura Kaminker et Simeon Kanev, « Private Sector Video Surveillance in Toronto: Not Privacy Compliant! », *Proceedings of the 2012 iConference,* New York, ACM, 2012, p. 354-362 ; et Sean P. Hier, *Panoptic Dreams: Streetscape Video Surveillance in Canada* (Vancouver, University of British Columbia Press, 2010).

3 Voir Brenda McPhail, Joseph Ferenbok, Roxanna Dehghan et Andrew Clement, « 'I'll Be Watching You': What Do Canadians Know About Video Surveillance and Privacy? », *iConference 2013 Proceedings,* iSchools, 2013, p. 555-559, https://www.ideals.illinois.edu/bitstream/handle/2142/39966/276.pdf?sequence=5.

4 Andrew Clement, Joseph Ferenbok, Roxanna Dehghan, Laura Kaminker, Simeon Kanev et Silvia Valdman, *Un détective privé « intelligent » dans les lieux publics ? L'analyse par vidéosurveillance, les nouvelles menaces à la vie privée et les solutions de rechange pour la protection des renseignements personnels,* rapport final, 23 juillet 2011, présenté au Commissariat à la protection de la vie privée du Canada, http://www.priv.gc.ca/resource/cp/2010-2011/p_201011_01_f.asp, p. 5.

5 Sur le « formatage d'information », voir Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York, Basic Books, 1988).

6 Voir Margaret E. Fulton, *La micro-électronique au service de la collectivité,* Rapport du Groupe de travail sur la micro-électronique et l'emploi (Ottawa, Travail Canada, 1982), p. 89. La surveillance en milieu de travail est devenue un enjeu des négociations collectives des trieurs de courrier à Postes Canada (Syndicat des travailleurs et travailleuses des postes), des agents de réservation d'Air Canada (Section locale unifiée nationale des travailleurs du transport aérien) et des téléphonistes de Bell Canada (Syndicat canadien des communications, de l'énergie et du papier).

7 Pour plus de renseignements sur le scandale, se reporter à l'article « British Phone Hacking Scandal (Leveson Report) », *New York Times*, http://topics.nytimes.com/top/reference/timestopics/organizations/n/news_of_the_world/index.html.

8 David Lyon, *Identifying Citizens: ID Cards as Surveillance* (Oxford, Polity Press, 2009).

9 On entend par « blanchiment politique » la pratique par laquelle les gouvernements nationaux incitent des organes internationaux à adopter une réglementation ; souvent cette réglementation est adoptée sans regard démocratique. Les gouvernements poussent ces organismes afin de procéder à des changements stratégiques qui seraient vraisemblablement impossibles au moyen des procédures législatives nationales. Voir Ian Hosein, « International Relations Theories and the Regulation of International Dataflows: Policy Laundering and Other International Policy Dynamics », document présenté à la réunion annuelle de l'Association des études internationales, Montréal, 17 mars 2004, http://citation.allacademic.com/meta/p_mla_apa_research_citation/0/7/3/8/8/pages73882/p73882-1.php ; et Barry Steinhardt, « Problem of Policy Laundering », American Civil Liberties Union, 13 août 2004, http://26konferencja.giodo.gov.pl/data/resources/SteinhardtB_paper.pdf.

10 Passeport Canada a finalement annoncé qu'à compter du 1er juillet 2013, *tous les nouveaux passeports canadiens délivrés sont des passeports électroniques*. Voir Canada, Passeport, À propos

des passeports électroniques, dernière modification le 9 août 2013, http://www.ppt.gc.ca/eppt/about.aspx?lang=fra.

11 Ces administrations sont la Colombie-Britannique, le Manitoba, l'Ontario, le Québec, le Vermont, New York, le Michigan et Washington. Voir la carte sur le site http://www.getyouhome.gov/html/EDL_map.html. Plusieurs autres provinces, dont la Saskatchewan et la Nouvelle-Écosse, ont également envisagé d'adopter le permis Plus, mais y ont renoncé. La demande a été plus faible que prévu et le permis ne semble pas avoir diminué la congestion aux frontières. Voir Gouvernement de la Saskatchewan, « Saskatchewan Halts New Enhanced Driver's Licence Program », Communiqué de presse du 23 mars 2009, http://www.gov.sk.ca/news?newsId=88eb5109-3361-4c9f-bafc-d4c226f5b897 et « Sask. Government Ditches 'Enhanced' Driver's Licence Plan », *CBC News,* 23 mars 2009, http://www.cbc.ca/news/canada/saskatchewan/sask-government-ditches-enhanced-driver-s-licence-plan-1.808226. Pour la Nouvelle-Écosse, voir « New Driver's Licence and Identification Cards », *Access Nova Scotia,* http://www.novascotia.ca/snsmr/access/drivers/new-licence.asp.

12 La norme appliquée à la puce d'identification par radiofréquence pour le permis de conduire Plus est la EPC Gen 2, qui la formulation abrégée de EPCglobal UHF Class 1 Generation. Pour un aperçu, des enjeux relatifs à la sécurité et à la protection de la vie privée soulevés par cette puce, se reporter à Wikipedia, dernière modification le 12 octobre 2013 http://en.wikipedia.org/wiki/Radio-frequency_identification#EPC_Gen2 *(en anglais seulement).*

13 Brenda McPhail, Krista Boa, Joseph Ferenbok, Karen Louise Smith et Andrew Clement, « Identity, Privacy and Security Challenges with Ontario's Enhanced Driver's Licence », *2009 Toronto International Conference, Science and Technology for Humanity (TIC-STH)*, Toronto, Ontario, 26-27 septembre 2009, IEEE Xplore Digital Library, 2009, p. 904-909, doi: 10.1109/TIC-STH2009.5444399.

14 *REAL ID Act of 2005*, Pub. L. 109-13, http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/html/PLAW-109publ13.htm.

15 Andrew Clement, Krista Boa, Simon Davies et Gus Hosein, « Toward a National ID Card for Canada? External Drivers and Internal Complexities », dans Colin J. Bennett et David Lyon (dir.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (Londres et New York, Routledge, 2008), p. 233-250.

16 « Insurance Corporation Offers to Help ID Rioters », *CBC News,* 18 juin 2011, http://www.cbc.ca/news/canada/british-columbia/story/2011/06/18/bc-icbc-rioters-id.html.

17 Un pixel invisible (pixel espion ou GIF invisible) est une image GIF invisible, de la taille d'un pixel, insérée dans une page Web ou un courriel en HTML, qui s'active lors du téléchargement de la page, lance une requête au serveur qui collectera des informations sur l'internaute à son insu, lesquelles seront transmises à un serveur distant pour exploitation ultérieure, notamment par des agences de marketing, http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367061.

18 En tentant de rejeter une plainte d'atteinte à la vie privée d'un consommateur, Google a eu recours au jugement dans l'affaire *Smith* c. *Maryland*, selon lequel une personne ne peut avoir une attente légitime de protection de la vie privée pour des renseignements qu'il a lui-même fournis à des tiers (*Smith* c. *Maryland* 442 U.S. 735, 743-44). Se reporter à « Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint » (affaire 5:13-md-02430-LHK, document 44, déposé le 13 avril 2013, au tribunal de district des États-Unis, district nord de la Californie, division San Jose), http://www.consumerwatchdog.org/resources/googlemotion061313.pdf, p. 19.

19 Pour en savoir plus sur le projet DeepPacketInspection.ca, consulter le http://www.deeppacketinspection.ca/.

20 Canada, Conseil de la radiodiffusion et des télécommunications canadiennes, *Politique réglementaire de télécom CRTC 2009-657 ; Examen des pratiques de gestion du trafic Internet des fournisseurs de services Internet*, Ottawa, 2009, http://www.crtc.gc.ca/fra/archive/2009/2009-657.htm.

21 Canada, Commissariat à la protection de la vie privée, *Projet d'inspection approfondie des paquets*, http://www.priv.gc.ca/information/research-recherche/dpi_index_f.asp.

22 British Columbia, Civil Liberties Association, *BCCLA Denounces Blocking of Website by Telus*, 26 July 2005, http://web.archive.org/web/20060101100357/http://www.bccla.org/pressreleases/05telus.htm.

23 Helmi Noman et Jillian C. York, *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010–2011*, OpenNet Initiative, mars 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011.

24 Voir Electronic Frontier Foundation, « NSA Spying on Americans », sans date, https://www.eff.org/issues/nsa-spying.

25 Également appelée *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, www.intelligence.senate.gov/laws/pl110261.pdf.

26 Une exception notable est l'affaire *Al Haramain Islamic Foundation* c. *Obama*, dans laquelle le demandeur a pu surmonter l'obstacle du secret d'État, mais a été débouté en 2012 en raison du fondement juridique technique de l'immunité absolue. Voir Electronic Frontier Foundation, « Al Haramain v. Obama », sans date, https://www.eff.org/cases/al-haramain.

27 James Ball, « NSA's Prism Surveillance Program: How It Works and What It Can Do », *The Guardian*, Royaume-Uni, 8 juin 2013, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

28 Le sous-marin nucléaire, USS *Jimmy Carter,* a été spécialement modifié pour mener des activités de branchement aux câbles sous-marins. Voir « New Nuclear Sub Is Said to Have Special Eavesdropping Ability », *New York Times*, 20 février 2005, http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=1&.

29 Ron Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, McClelland and Stewart, 2013), p. 43. Voir aussi Andrew Clement, « IXmaps—Tracking Your Personal Data Through the NSA's Warrantless Wiretapping Sites, » *2013 IEEE International Symposium on Technology and Society (ISTAS),* Toronto, 27–29 juin 2013 (IEEE Xplore Digital Library, 2013), p. 216–223, doi: 10.1109/ISTAS.2013.6613122.

30 Voir Meagan Fitzpatrick, « Online Surveillance Bill Could Change, Harper Signals », *CBC News*, 15 février 2012, http://www.cbc.ca/news/politics/online-surveillance-bill-could-change-harper-signals-1.1150295 ; et le titre initial du projet de loi était la *Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois*, (2012) ; pour le texte complet, consulter le http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5380965&file=4.

31 Phillipa Lawson, *Moving Toward a Surveillance Society: Proposals to Expand "Lawful Access" in Canada*, BC Civil Liberties Association, 2012, http://bccla.org/wp-content/uploads/2012/03/2012-BCCLA-REPORT-Moving-toward-a-surveillance-society1.pdf, p. 5.

32 Ibid.

33 Anna Mehler Paperny, « Telcos in Talks with Ottawa to Shape Internet 'Spy' Bill: Documents », *Globe and Mail*, 29 juin 2012, http://m.theglobeandmail.com/technology/tech-news/telcos-in-talks-with-ottawa-to-shape-internet-spy-bill-documents/article4376958/?service=mobile.

34 La Coalition Arrêtez l'espionnage en ligne compte de nombreux membres partout au Canada et a été organisée par OpenMedia.ca. Se reporter à https://openmedia.ca/fr/ArretezLEspionnage.

35 Voir, par exemple, la vidéo « (Un)Lawful Access: Canadian Experts on the State of Cyber-surveillance », 2011, http://unlawfulaccess.net/.

36 John Ibbitson, « Harper Government Kills Controversial Internet Surveillance Bill », *Globe and Mail*, 11 février 2013, http://www.theglobeandmail.com/news/politics/harper-government-kills-controversial-internet-surveillance-bill/article8456096/.

37 Leo Singer, « Accès excessif ? », *National : actualités et tendances en droit*, Association du Barreau canadien, juin 2012, http://www.nationalmagazine.ca/Articles/June-2012-Issue/Unwarranted-access.aspx.



Prendre le virage biométrique

De la surveillance corporelle à la surveillance intracorporelle

La porte d'une salle de cours à l'Université de l'Arizona s'ouvre lentement. Un coffre futuriste est poussé à l'intérieur puis une équipe méticuleuse de scientifiques, d'administrateurs et d'étudiants aux cycles supérieurs font leur entrée. Le coffre est ouvert et une machine qui ressemble à un guichet automatique bancaire en est minutieusement retirée. On appuie sur quelques boutons puis on fait certaines mises au point ; c'est alors que la machine « s'éveille ». Sur l'écran, on peut voir un visage humain créé par ordinateur ; les yeux de l'homme clignent et il regarde des deux côtés. AVATAR est prêt. AVATAR, signifie en anglais *Automated Virtual Agent for Truth Assessments in Real-Time* ou agent virtuel automatisé d'évaluation de la vérité.

L'agent pose toutes les questions qu'un voyageur se ferait habituellement poser à la frontière ; il demande si le voyageur a fait lui-même ses bagages, où il compte séjourner et la durée prévue du voyage. La différence est que tout le processus de vérification est fait par AVATAR, une borne dotée de capacités biométriques et d'une intelligence artificielle qui est chargée de déterminer si les voyageurs doivent ou non faire l'objet d'une inspection subséquente. AVATAR est censé détecter la supercherie, que ce soit un mensonge en réponse à une question, de la contrebande ou un éventail d'autres infractions possibles.

La démonstration d'AVATAR qui a été faite en septembre 2010 était précédée d'une conférence du professeur Nunamaker, chef du projet AVATAR

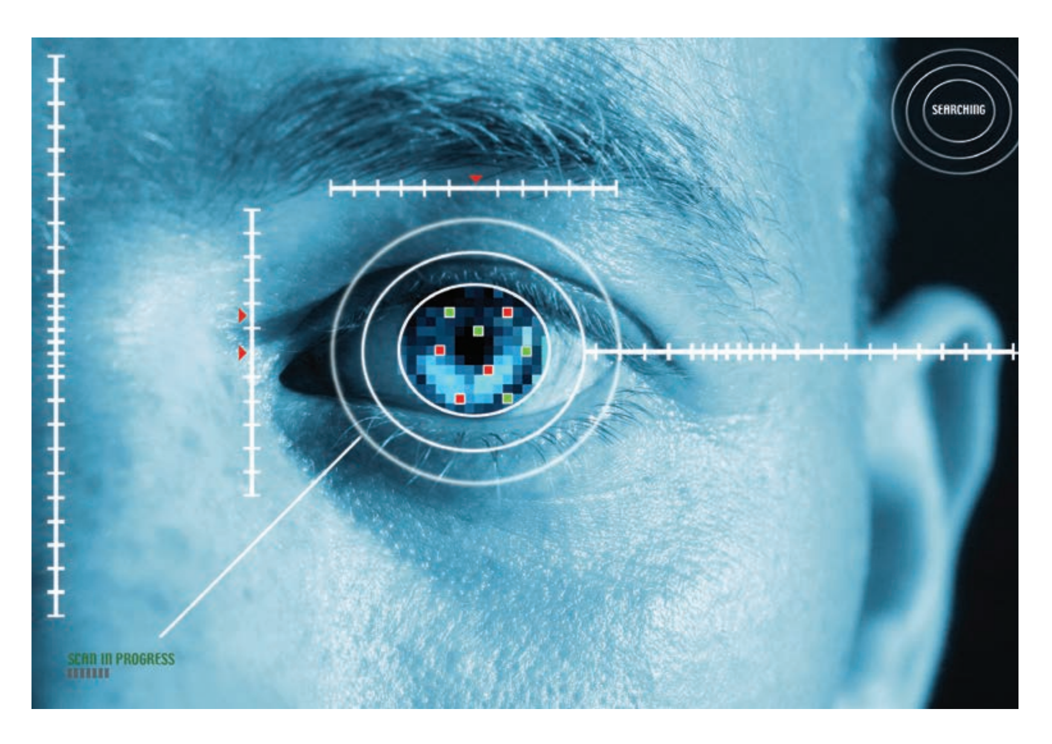
et professeur au département des systèmes d'information de gestion à l'Université d'Arizona. Dans son exposé, M. Nunamaker a vanté les capacités d'AVATAR, de même que celles de SPECIES (*Special Purpose Embodied Conversational Intelligence with Environmental Sensors* ou intelligence interactive personnifiée à usage déterminé avec des capteurs environnementaux embarqués). SPECIES est le modèle technologique à la base d'AVATAR, lequel est en soi un exemple de ce que l'on appelle généralement un agent interactif personnifié. Bien que l'AVATAR soit un exemple à l'extrême (et un exemple étatsunien), il illustre une série de tendances et de croyances qui devraient intéresser les Canadiens ou peut-être même les bouleverser. Cet exemple témoigne, entre autres, de la croyance selon laquelle la technologie est neutre, efficace et presque infaillible et qu'elle peut faire mieux que les gens sur lesquels nous comptions auparavant pour protéger nos frontières et pour vérifier notre fiabilité. Cependant, comme toutes les technologies, AVATAR a été fabriqué par des humains et repose sur des hypothèses humaines relatives aux comportements, à la race, au sexe, aux tromperies, etc. Les technologies comme celle-ci ne sont pas neutres, car elles prennent appui sur les hypothèses et les préjugés de leurs créateurs[1].

L'une de ces hypothèses a trait au genre. Selon la plupart des protocoles de passage à la frontière, on suppose qu'une personne est soit homme, soit femme. Or, cette simple supposition expose les transgenres à un risque puisque l'image qu'ils présentent ne correspond pas aux genres consignés dans les bases de données officielles. Les données et la technologie qui prend les décisions au sujet de personne en fonction de ces données ne sont pas neutres. Elles sont plutôt l'incarnation d'hypothèses discriminatoires au sujet de l'identité humaine.

Quelles sont les technologies biométriques ?

La neutralité des technologies est une croyance à la base de nombre de technologies biométriques. Cette croyance est également répandue chez les fonctionnaires, les décideurs et les agents d'exécution de la loi des deux côtés de la frontière canado-américaine.

Les systèmes biométriques transposent les caractéristiques physiologiques en format numérique. Ils peuvent prendre la forme de simples lecteurs numériques d'empreintes digitales, qui sont généralement très fiables et peu coûteux, de lecteurs de rétine ou d'iris, ou de systèmes complexes qui



Les lecteurs de l'iris sont une mesure de sécurité répandue (Source : © iStockphoto.com/tlnors)

mesurent la température corporelle, l'odeur ou la démarche. Cette technologie semble évoluer vers l'intelligence artificielle, les prothèses et les corps virtuels. Le recours croissant aux multiples techniques de surveillance corporelle semble aller de pair avec l'obsession bio-politique contemporaine du gouvernement et du secteur privé, qui les pousse vers la planification d'interventions sociales variées pour modifier le taux de natalité, de récidive, de décès, d'incarcération, etc.

Les analystes et les citoyens engagés qui souhaitent mieux connaître les technologies actuelles et futures de surveillance auront peut-être du mal à comprendre ces nouveautés. Pour ce faire, ils devront comprendre la distinction cruciale entre l'authentification et l'identification. L'identification consiste à savoir qui vous êtes en tant que personne unique, mais un organisme peut *authentifier* une personne comme un bénéficiaire légitime d'un service sans connaître l'identité réelle de cette personne. On pouvait lire dans un rapport de recherche sur la biométrie publié récemment par le National Research Council aux États-Unis que :

La biométrie au port d’Halifax

En 2007, on a annoncé qu’un contrat venait d’être attribué à Unisys pour la mise au point et la gestion d’un système biométrique qui permettrait de contrôler l’accès de quelque 4 000 travailleurs au port d’Halifax. Le projet a été réalisé conformément à la *Loi sur la sûreté du transport maritime* de Transport Canada. Le système repose sur la reconnaissance de la vascularisation de la main (HVPR) mise au point par Identica. Un balayage au moyen de rayons infrarouges est effectué sur le dos de la main du travailleur puis intégré à une carte intelligente, sur laquelle on retrouve également la photo du détenteur[1].

Cette image vasculaire reconnue par un capteur à infrarouge est utilisée pour identifier le titulaire de la carte lorsque celui-ci la présente et place le dos de sa main sur le lecteur. La vérification se fait instantanément et est complétée si la vascularisation de la main du détenteur correspond à celle qui a été enregistrée sur la carte. L’attribut biométrique est stocké seulement sur la carte et non dans une base de données. Le système sert à limiter l’accès et à permettre l’entrée aux zones sécurisées seulement aux travailleurs qui ont les autorisations requises. Les

> [Traduction] Les technologies d’authentification reposent généralement sur l’un des trois éléments suivants : une chose que la personne sait, comme un mot de passe ; une chose que la personne possède, comme une clé ou un jeton sécurisés ; ou une chose que la personne est ou fait. Les technologies biométriques sont fondées sur le dernier de ces éléments. Contrairement aux systèmes utilisant des mots de passe ou un jeton, les systèmes biométriques peuvent fonctionner sans que l’utilisateur n’ait à intervenir, sans qu’il ne coopère, sans même qu’il ne sache que la reconnaissance a lieu[2].

Autrement dit, les technologies biométriques ne visent pas à remplacer d’autres systèmes d’authentification. Elles visent plutôt à les bonifier dans un environnement de sécurité fondé sur l’abondance de données. Cependant, la capture passive de renseignements suscite certaines préoccupations au sujet de la fiabilité réelle de ces technologies et de notre capacité ou de notre incapacité à protéger ou contrôler la capture, l’échange et le transfert de ces renseignements personnels.

travailleurs doivent également utiliser la carte et vérifier leur identité lorsqu'ils quittent une zone. Plus de 60 lecteurs ont été installés au port depuis 2008.

Le système HVPR est vendu comme un exemple de la nouvelle génération de systèmes d'authentification biométrique; exemple de Protection intégrée de la vie privée ou PIVP, il est plus fiable et plus sûr que les technologies biométriques précédentes et est muni de fonctions permettant de mieux protéger les renseignements personnels. Depuis le 11 septembre, les ports sont des cibles majeures et méritent des systèmes de sécurité à la fine pointe de la technologie. Ces mesures sont-elles une réaction proportionnelle et justifiée à une préoccupation réelle sur le plan de la sécurité? Ou sont-elles exagérées, trop coûteuses, portant atteinte à la vie privée et en définitive, inefficaces?

1. Voir L. Samuel Pfeifle, « Unisys' Hand-Scan Plan », *Security Systems News*, 1 octobre 2007, p. 19-20; T. Peters, « Halifax to Use Biometrics to Identify Port Workers », *Canadian Sailings*, 3 septembre 2007, p. 15; et « Halifax Port Security to Scan Veins in Hands », *CBC News*, 7 septembre 2007, http://www.cbc.ca/news/canada/nova-scotia/halifax-port-security-to-scan-veins-in-hands-1.665612.

La surveillance corporelle n'est limitée que par l'imagination humaine. Elle a fait son apparition dans plusieurs domaines. Dans les écoles canadiennes, on utilise les empreintes digitales des enfants pour les systèmes de paiements sans numéraire[3]. Au parc aquatique Calypso à Ottawa, on utilise les empreintes digitales pour le paiement de l'entrée et plusieurs entreprises envisagent d'installer ou ont déjà installé des systèmes conçus pour faire le suivi des heures de travail, du temps supplémentaire et des retards des employés au moyen des empreintes digitales[4]. Au port d'Halifax, les travailleurs doivent présenter le dos de leur main pour un balayage afin d'avoir accès au port[5]. Comme pour les stratégies de sécurité frontalière, ces mesures font intervenir un amalgame complexe de mécanismes privés et publics. Si on la conjugue aux gains d'efficacité présumés, la promesse de renforcement de la sécurité – bien qu'elle ne s'appuie souvent sur aucune preuve concrète – semble, à de rares exceptions près, suffire pour que les propriétaires d'entreprise, les décideurs et les actionnaires adhèrent à la surveillance biométrique.

La biométrie à la frontière : un exemple de la biométrie à l'œuvre

Comme le montrent diverses ententes et initiatives bilatérales (particulièrement celles établies depuis le 11 septembre), il semble que tous les paliers de gouvernement au Canada soient de plus en plus enclins à adopter les technologies biométriques et les techniques de surveillance corporelles conçues ou utilisées aux États-Unis. De plus, ces gouvernements sembleraient accepter davantage les initiatives visant à partager de grandes quantités de données et d'information personnelle avec les États-Unis. Et, souvent, toutes ces initiatives sont prises sans qu'un débat public ait lieu et sans attirer l'attention des médias.

La plupart des gens connaissent mieux la surveillance dite corporelle depuis les attentats du 11 septembre 2001. Or, les emplois de la biométrie vont bien au-delà de la lutte contre le terrorisme. En effet, toutes les formes de surveillance sont depuis longtemps associées au maintien de la productivité et de la sécurité au sein de la population[6]. En parallèle, la prédominance dans les politiques gouvernementales de la privatisation, de la déréglementation et du renforcement des pouvoirs du marché a contribué à favoriser tant la libre circulation des capitaux qu'une intensification de l'individualisme. Ensemble, ces facteurs ont créé les conditions idéales à la montée de la surveillance corporelle.

En faisant un examen rapide des politiques de sécurité dans les aéroports, on découvre qu'une série d'acteurs sont chargés de fonctions qui souvent se chevauchent et s'embrouillent. Parmi lesdits acteurs, mentionnons la GRC et les services de police locaux, les commissaires et les agents de sécurité privés, les entrepreneurs embauchés par l'Administration canadienne de la sûreté du transport aérien (ACSTA) qui participent à la vérification préalable des passagers et les agents de l'Agence des services frontaliers du Canada (ASFC) qui sont maintenant autorisés à porter une arme. Les employés des transporteurs aériens s'insèrent également dans ce réseau de gestion de la sécurité puisque certaines fonctions de sécurité, comme l'application des listes d'interdiction de vol, ont été déléguées aux compagnies aériennes. À cette image déjà complexe il faut encore ajouter le réseau de caméras de surveillance, y compris les responsables de sa gestion et de sa maintenance, les lecteurs de passeport électroniques, les scanneurs corporels et les bornes de services pour les voyageurs, qui représentent tous leurs concepteurs privés ou publics.

Ces dispositifs et ces pratiques sont utilisés sous divers modèles d'administration de la sécurité et ont pour base des notions de risque, de menace

et de danger très diverses. Ils font également intervenir différentes applications de la surveillance corporelle, qui sont toutes reliées d'une manière complexe de sorte qu'il est difficile d'adopter un point de vue critique face à ces avancées. Ces difficultés sont aggravées par le fait que ces systèmes fonctionnent dans des emplacements, comme des aéroports, où les pouvoirs discrétionnaires de l'État s'affermissent pour des raisons de sécurité.

La technologie biométrique que le Canadien moyen connaît le mieux est sans doute le scanneur corporel, qui est maintenant utilisé dans les grands aéroports canadiens. Ces scanneurs ont été installés après que Umar Farouk Abdulmtallab eut tenté de faire exploser son caleçon-bombe dans un vol Amsterdam-Detroit le 25 décembre 2009. La tentative d'Abdulmtallab avait cependant avorté grâce à des passagers vigilants et non grâce aux scanneurs de sécurité. Néanmoins, le 5 janvier 2010, les Canadiens ont appris que des scanneurs corporels seraient installés dans les principaux aéroports. De plus, on mettrait à l'essai de nouvelles techniques d'observation du comportement (décrites dans ce qui suit) à l'aéroport international de Vancouver au cours de l'année suivante. Bien que les scanneurs corporels aint frappé l'imaginaire de nombreux Canadiens, plus particulièrement de ceux qui s'inquiétaient de la possibilité que les agents de sécurité les voient nus, l'annonce de l'initiative d'observation du comportement a été suivie d'un silence radio.

Les scanneurs corporels dirigent des ondes radio millimétriques sur le corps qui, lorsqu'elles sont reflétées, produisent une image en trois dimensions. Ces machines sont censées montrer des objets comme des armes ou des explosifs qu'un voyageur pourrait cacher sous ses vêtements. L'idée était de donner aux passagers le choix entre une fouille manuelle – par palpation – et les nouveaux scanneurs. Ces dispositifs sont maintenant bien connus des voyageurs aériens et nombre d'entre eux les ont déjà expérimentés. Malgré le débat public sur la violation possible de l'intimité que pourraient constituer les images produites et sur les personnes qui pourraient voir ces images et en dépit d'appréhensions persistantes, on semble avoir apprivoisé les scanneurs corporels et les considérer maintenant comme normaux. De plus, le Commissariat à la protection de la vie privée du Canada s'est dit satisfait de l'évaluation des facteurs relatifs à la vie privée fournie par l'ACSTA.

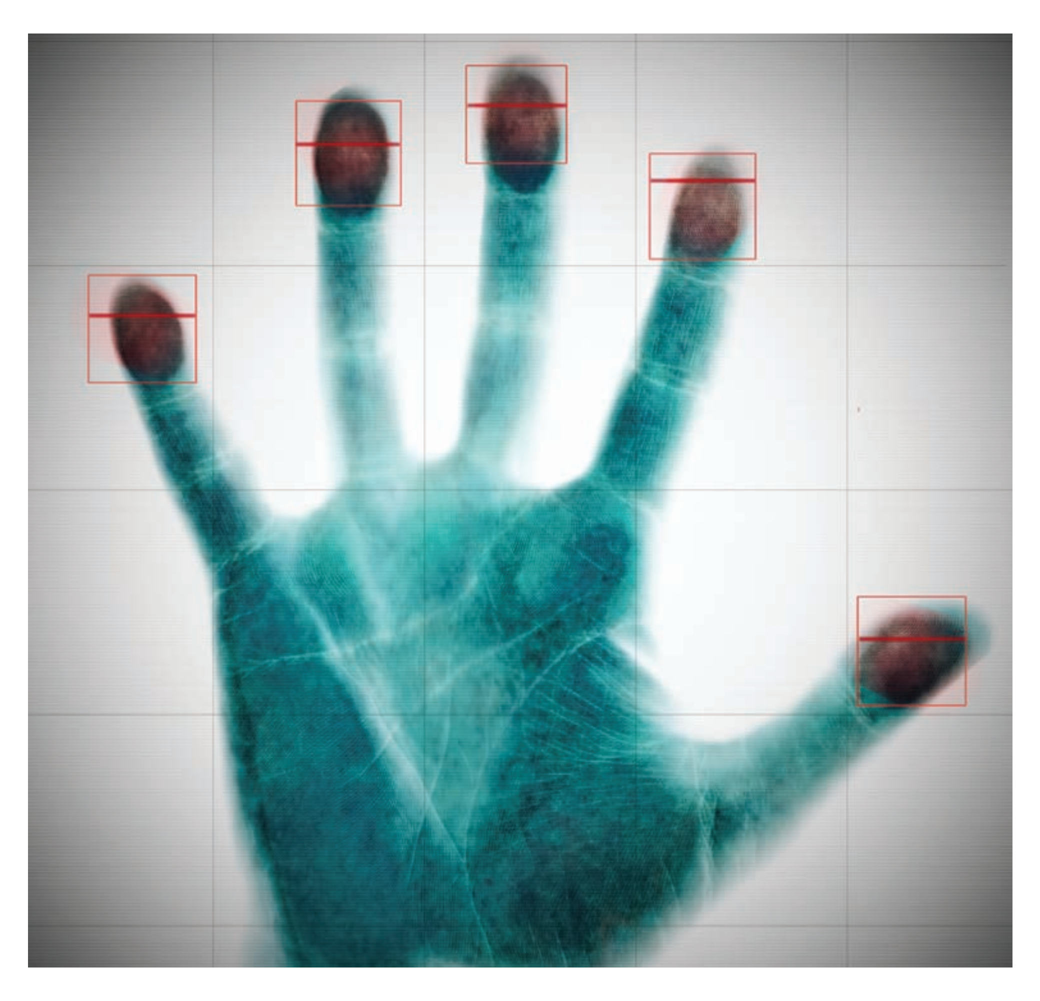
L'observation du comportement est une pratique qui est utilisée depuis de nombreuses années à l'aéroport Ben Gurion à Tel-Aviv. Si les autres formes de surveillance visent à chercher des *objets* potentiellement dangereux, la surveillance par l'observation du comportement est censée permettre de repérer les *personnes* potentiellement dangereuses. Au Canada, de février à

juillet 2010, des agents spéciaux en civil ont observé les passagers aux portes d'embarquement à l'aéroport international de Vancouver pour repérer les comportements suspects. Ce passager semble-t-il nerveux ? Transpire-t-il ? Tape-t-il du pied ? Est-il trop habillé malgré la chaleur ? Le cas échéant, le passager était interrogé par les agents. Cela soulève de nouveaux enjeux relatifs à la formation des agents et à l'identification erronée de personnes « suspectes ». L'enjeu le plus alarmant est sans doute la possibilité que du profilage soit effectué en fonction du groupe ethnique, de l'âge ou du sexe pour déterminer quels passagers semblent suspects[7]. La commissaire fédérale à la vie privée se penche actuellement sur la question[8].

Engouement passager pour la biométrie

Bien que nombre de technologies servent à la surveillance corporelle, les technologies biométriques en sont la forme la plus évidente et la plus courante de nos jours. Le faible coût des systèmes biométriques est l'un des facteurs ayant contribué à leur prévalence, mais ce n'est pas le seul. En effet, force est de constater que, depuis les attentats terroristes du 11 septembre, bureaucrates et responsables de tout genre assimilent volume élevé de données à renforcement de la sécurité. Les attentats en soi ont été perçus comme un effondrement des capacités de l'État à évaluer, prévoir et répondre adéquatement aux risques de terrorisme, une incapacité qui a été attribuée essentiellement à un manque de données. Autrement dit, on semble être obsédé actuellement par une conception selon laquelle la surveillance et les systèmes de collecte de données renforcent, en soi, la sécurité. L'hypothèse douteuse selon laquelle un manque de données est dangereux s'est alors transformée en un motif convaincant pour augmenter le recours aux systèmes biométriques et à d'autres formes de surveillance corporelle qui génèrent une avanlanche de données. Enfin, les décisions prises par les gouvernements pour gérer les populations, même celles prises aux frontières – là où les pouvoirs discrétionnaires de l'État atteignent leur apogée – débordent souvent dans le secteur privé.

On ne peut faire de distinction claire entre l'utilisation d'attributs biométriques dans les passeports pour protéger les frontières des voyageurs indésirables, les cartes d'identité biométriques servant à contrôler et les déplacements des employés de l'ACSTA dans les zones réglementées des aéroports canadiens ou les systèmes biométriques employés par l'Administration



La lecture biométrique d'empreintes digitales dans un système de sécurité (Source : © iStockphoto.com/malexeum)

portuaire d'Halifax pour surveiller les travailleurs du port. En effet, la gestion des populations, qu'elle vise à contrôler le passage aux frontières ou les retards au travail, est un bon exemple de la distinction trouble entre le privé et le public (se reporter à la Tendance 3). Souvent les adeptes de ces systèmes, prétextant un présumé penchant naturel de l'être humain pour l'efficacité, les présentent comme un outil qui facilite notre mobilité. Or, comme par hasard, ils ne disent pas à quel point cet outil peut *diminuer* la mobilité de certains groupes et entraîner une application très rigoureuse des pouvoirs aux frontières ou en milieu de travail. Ces systèmes pourraient même priver

À l'école sans monnaie

Les techniques biométriques sont rapidement passées des aéroports, des prisons et des environnements militaires aux établissements civils de tous les jours; en effet, les écoles secondaires semblent vouloir se métamorphoser en laboratoires de surveillance[1]. Dans le cadre de l'initiative Cashless Schools (écoles sans espèces), l'école secondaire de Fredericton au Nouveau-Brunswick permet maintenant aux élèves de payer leur repas à la cafétéria au moyen d'une empreinte de leur pouce. Ces systèmes se vendent beaucoup au Canada, tant aux universités qu'aux écoles secondaires. Dans le cas de cette école secondaire, les parents doivent s'inscrire auprès de Cashless Schools (entreprise canadienne qui se spécialise dans les systèmes de paiement pour les écoles), faire un dépôt dans leur compte et signer un formulaire de consentement pour confirmer que leur enfant peut utiliser le lecteur biométrique.

Les étudiants doivent enregistrer une empreinte digitale dans le système pour pouvoir faire des achats sans espèces. Les renseignements consignés dans la base de données sont utilisés pour faire la vérification au moment de l'achat, soit à la cafétéria. Bien que l'entreprise Cashless

d'un droit les personnes qui ne seraient pas admissibles à certains programmes puisqu'il leur manque par exemple la partie du corps associée au lecteur (iris, cinq doigts à une main ou empreintes digitales lisibles).

L'évolution technique de la sécurité frontalière et de tout un éventail d'autres domaines modernes de sécurité au cours des dix dernières années a contribué à ce recours croissant aux systèmes biométriques. La notion selon laquelle la visibilité est accrue par la capture biométrique d'un attribut du corps (la conception selon laquelle le corps est un mot de passe) est directement liée à la tendance à adopter de plus en plus de mécanismes de sécurité s'appuyant sur une quantité encore plus grande de données. Plus le recours aux divers mécanismes de collecte directe de renseignements humains, tels que l'interaction avec un garde-frontière ou un agent des douanes, diminue, plus le recours à l'évaluation préalable du profil des personnes qui tentent de traverser la frontière augmente. Le même phénomène peut être observé pour les acheteurs, les clients, les consommateurs, etc. Ces évaluations préalables peuvent être effectuées au moyen de systèmes de présélection des passagers utilisés au moment de l'achat du billet d'avion[9], ou au moyen de systèmes pour les voyageurs qui dépendent de données issues de profils particuliers,

Schools rassure les clients en assurant qu'elle surpasse les normes en matière de renseignements personnels et de sécurité, il faut dire que les usages possibles des systèmes biométriques dans les écoles pourraient s'étendre à bien d'autres domaines.

Dans d'autres contextes, les parents ou les responsables des soins médicaux dans les écoles peuvent vérifier les repas achetés au moyen de la lecture de l'empreinte digitale. Certains élèves pourraient bien se voir interdire d'acheter de la pizza ou un hamburger ! Certaines écoles qui ont installé des systèmes biométriques prévoient maintenant utiliser les lecteurs pour les autobus scolaires, la bibliothèque et le stationnement. Le glissement de la surveillance semble être logique sur le plan économique et technique; si le système offre ce potentiel, pourquoi ne pas en profiter? On ne semble pas se soucier de la nécessité du système, de son efficacité ou du fait qu'il soit adapté ou non à l'activité ni même de trouver une solution de rechange qui porterait moins atteinte à la vie privée.

1. John Gilliom et Torin Monahan, *Supervision: An Introduction to the Surveillance Society* (Chicago, University of Chicago Press, 2013), p. 73.

comme le programme NEXUS (le programme qui facilite le passage des voyageurs à la frontière canado-étatsunienne). Ces systèmes permettent de calculer à quels voyageurs on peut faire confiance et permettre de voyager avec un minimum de supervision. Comme l'ensemble des données personnelles de l'individu, aussi appelé « double de données »[10], est fréquemment distribué parmi un vaste éventail d'organismes souhaitant confirmer l'identité de cette personne, on prétend qu'il est maintenant essentiel de convertir la physionomie de cette personne en un algorithme visible et lisible à la machine. Ces mesures sont devenues synonymes de renforcement, d'intensification et d'augmentation présumée de l'efficacité et de l'efficience de la sécurité. Elles illustrent également la conclusion tirée par Toby Miller : la contrepartie de la sécurité fournie par le gouvernement est que nos vies (ainsi que nos corps) doivent être connaissables[11].

On promet un renforcement de la sécurité en échange de cette visibilité. D'ailleurs, les autorités ont stratégiquement recadré les événements du 11 septembre survenus à Washington, à New York et en Pennsylvanie comme un reflet de l'insécurité extrême et de l'imprévisibilité de la vie moderne et les ont attribués à une défaillance catastrophique des infrastructures existantes

de sécurité. Elles ont présenté cette insécurité comme si une défaillance systémique à proprement parler ne pouvait en être la cause. Elles ont donc attribué cette insécurité à une fraude ou à une tromperie opérée sur l'infrastructure de sécurité et d'identité en place. Par conséquent, les mesures prises par la suite ont été axées sur la vérification et l'authentification de l'identité ; autrement dit, on souhaite avoir la certitude que vous êtes bien qui vous dites être. Cette quête est aujourd'hui synonyme de l'avènement de la surveillance corporelle puisque les méthodes traditionnelles d'authentification comme le passeport ou d'autres certificats d'identité ont manifestement échoué par le passé. La question « êtes-vous bel et bien qui vous dites être ? » peut sembler bizarre, mais elle a le mérite d'être directe ; elle a également entraîné la mise en œuvre de toute une panoplie de pratiques, de techniques et de technologies visant à accroître la visibilité et à renforcer les capacités de l'État à repérer et gérer les risques[12].

Nous avons donc pu observer une augmentation des dépenses en vue de confirmer que tous ceux qui traversent la frontière sont « visibles et connaissables ». De plus, lorsque cela est possible, les nouvelles mesures portent principalement sur l'évaluation préalable du risque. Voilà pourquoi un nombre toujours croissant de stratégies et de techniques gouvernementales ont servi à augmenter la quantité de données recueillies au moyen de la surveillance corporelle. Encore une fois, les comportements et les mesures de surveillance adoptés aux frontières ont été imités et reproduits dans d'autres secteurs. En effet, on inclut maintenant des attributs biométriques dans les systèmes de paiement simplifié, le suivi des employés et la gestion de l'accès à des installations publiques et privées. Tant dans le secteur privé que dans le secteur public, on tend à croire que ces mécanismes permettent une amélioration de l'efficacité et un renforcement de la sécurité. On utilise donc des systèmes biométriques au Canada pour payer le dîner de son enfant à l'école, pour entrer à la salle de conditionnement physique du quartier ou pour faire le suivi des employés d'un cabinet d'avocat[13].

La biométrie : où est le problème ?

Les responsables des politiques et les organes d'exécution de la loi de l'État font généralement la promotion de ces technologies d'authentification, malgré l'absence relative de données qualitatives et quantitatives pertinentes pour prouver leur efficacité. En fait, des rapports ont fait ressortir des

problèmes graves concernant la fiabilité et les taux élevés de « faux positifs » produits par les systèmes biométriques. Parmi ces faux positifs, citons les situations où une personne serait jugée à tort comme étant à risque ou celles où des personnes sont ajoutées par erreur à une liste de surveillance ou à une liste d'interdiction de vol[14]. Or, ces situations évidemment déconcertantes n'englobent pas les enjeux socio-culturels et politico-économiques plus vastes découlant du recours à ces technologies ; technologies qui nécessitent pour la plupart l'utilisation de systèmes de capture et d'évaluation préalable qui dépendent d'une quantité de données toujours plus grande[15]. Elles témoignent également d'une dépendance indue à des solutions techniques, en l'absence de recherche convaincante sur l'efficacité et les répercussions globales de leur utilisation[16].

Dans son analyse sagace sur la biométrie, Shoshana Magnet affirme avec concision que le corps humain n'est pas « biométrifiable »[17]. Cela, parce que le corps humain n'est simplement pas suffisamment statique pour que cette forme d'identification soit fiable, et ce, en dépit de tous les investissements colossaux réalisés pour la mise au point des technologies biométriques. Les sciences naturelles commencent à rejoindre cette analyse, acceptée depuis une dizaine d'années par les sciences humaines et sociales. Le rapport produit en 2012 par le National Research Council of National Academies, *Biometric Recognition*, ainsi que les recherches approfondies menées par l'Université Notre Dame[18] ont tous deux souligné les problèmes engendrés par la qualité dynamique des caractéristiques physiques que la biométrie prétend identifier. Citons par exemple que l'iris change avec l'âge. Certains doutes ont également été émis concernant la science sous-jacente qui permet de convertir la physionomie en algorithmes. En résumé, les auteurs du rapport du National Research Council indiquent que :

> [Traduction] Les utilisateurs et les développeurs des systèmes biométriques devraient admettre les limites et les contraintes des systèmes biométriques. Ils devraient tenir compte plus particulièrement de la nature probabiliste de la science sous-jacente, des limites actuelles des connaissances sur l'individualité humaine et des nombreuses sources d'incertitudes dans les systèmes biométriques[19].

Manifestement, ces propos ne reflètent pas le discours des professionnels de la sécurité, des décideurs et des responsables de la sécurité frontalière qui persistent à vanter les vertus des attributs biométriques, notamment des

passeports, des scanneurs corporels et des cartes des programmes pour les voyageurs dignes de confiance.

La communauté scientifique commence à s'interroger sur la biométrie. Ce questionnement pourrait constituer une occasion pour entamer un débat plus critique sur ces systèmes technologiques et sur leurs développeurs et leurs promoteurs respectifs, de la même façon dont les scientifiques ont fait état de préoccupations socio-politiques et éthiques cruciales au sujet d'autres technologies. Prenons le célèbre exemple de J. Robert Oppenheimer et des critiques qu'il a soulevées contre le Projet Manhattan. Physicien théoricien connu comme le père de la bombe atomique, Oppenheimer a été l'un des acteurs clés de la mise au point d'armes nucléaires pour les États-Unis vers la fin de la Seconde Guerre mondiale. Cependant, tout de suite après la guerre, Oppenheimer, en qualité de conseiller en chef de l'Atomic Energy Commission des États-Unis, a commencé à émettre des critiques véhémentes au sujet des armes nucléaires et s'est fait le défenseur de la non-prolifération tout en prônant un évitement de la course aux armements avec l'URSS. De la même manière, des scientifiques participant à la mise au point de la biométrie critiquent de plus en plus l'efficacité et la fiabilité de ces systèmes[20].

Conclusion

Alors que pouvons-nous faire ? Comment pouvons-nous, en tant que citoyens qui ont souvent été rendus plus vulnérables par l'intensification des pouvoirs de l'État et du secteur privé, interagir avec ces technologies et ces systèmes de surveillance qui reposent sur la surveillance corporelle tout en gardant un œil critique ? Malheureusement, il n'existe aucune recette en la matière. Il existe toutefois plusieurs possibilités pour qu'un citoyen engagé puisse soulever des questions importantes et puisse se familiariser avec les hypothèses, les promesses et les revendications souvent douteuses qui sont associées à la prédominance croissante de ces technologies. Bien que le virage vers la surveillance corporelle, particulièrement vers les systèmes biométriques, s'inscrive dans le cadre du culte technologique, il existe des facteurs systémiques plus profonds qui font en sorte que la mise en œuvre de ces systèmes semble logique. Citons tout d'abord l'adoption générale de la pratique de gouvernance par le risque[21] dont nous avons fait état dans la Tendance 2. Cette pratique fait intervenir des stratégies conçues pour atténuer les risques incalculables ou pour administrer l'ingérable.

Le fait que nombre de risques ne puissent être calculés et qu'ils sont par conséquent inconnus et impossibles à connaître est maintenant assimilé, dans l'esprit des planificateurs de la sécurité et d'un public de plus en plus inquiet, à un niveau intolérable d'insécurité et de danger. Une façon de donner à la population un sentiment de sécurité consiste à recueillir les données personnelles sur les membres d'un large éventail de groupes au moyen de systèmes variés. On estime que les personnes inscrites à ces systèmes – que ce soit un système pour les grands voyageurs, pour les voyageurs dignes de confiance, pour l'inscription aux passeports ou pour l'évaluation du crédit – sont plus facilement connaissables ; cette capacité de connaître a fini par être identifiée comme une forme de sécurité tant par l'État que par les entreprises. En conséquence, la logique de la gestion du risque a poussé les acteurs du secteur public et du secteur privé à accroître leurs connaissances sur la population en vue d'améliorer la sécurité. Enfin, les applications de la biométrie donnent l'illusion que les membres de ces populations sont bel et bien qui ils affirment être.

La gestion du risque est également populaire auprès des représentants du gouvernement, puisqu'elle constitue une façon de faire face aux pressions financières à une époque où l'austérité et les compressions se heurtent à une augmentation prétendument nécessaire des dépenses de sécurité et de surveillance. L'analyse de la gestion du risque est fondée sur des calculs ou sur des prévisions de la fréquence des risques et de leurs répercussions potentielles. Plus particulièrement, depuis le 11 septembre, elle sert à justifier l'augmentation des dépenses publiques et a entraîné une hausse spectaculaire des dépenses de sécurité. Au Canada, un peu moins de 100 milliards de dollars de *plus* ont été investis dans la sécurité nationale dans la décennie suivant ces attentats que si les dépenses avaient respecté les budgets établis avant les attentats. En revanche, près de 1 billion de dollars ont été dépensés pour la même période aux États-Unis[22]. Les bureaucrates et leurs maîtres politiques sont parvenus à faire croire que la fréquence possible et les répercussions potentielles de risques comme le terrorisme étaient plus importantes et nécessitaient plus d'investissements de la part du gouvernement que toute une série d'autres services et de postes budgétaires qui se disputent ces fonds restreints.

La nécessité d'adhérer à la surveillance corporelle en gardant un regard critique n'est pas une attaque contre les technologies elles-mêmes. Les jugements normatifs simplistes ne sont d'aucune utilité ici. Certains systèmes biométriques ne portent pas une grande atteinte à la vie privée, sont assortis

de mesures de protection des renseignements personnels robustes et servent efficacement les objectifs de sécurité et d'efficacité. Par ailleurs, il existe des utilisations appropriées et inappropriées de ces dispositifs. La carte d'identité de zone réglementée utilisée par l'ACSTA, dont nous avons parlé précédemment, sert simplement à sécuriser les zones non publiques dans les aéroports au moyen de vérifications aléatoires des personnes se trouvant dans ces corridors ou ces zones. Les renseignements biométriques de l'employé sont contenus dans cette carte. Au cours d'une vérification aléatoire, une correspondance est établie entre l'empreinte digitale encryptée sur la carte qui est passée dans le lecteur et l'empreinte digitale qui se trouve au moment même sur le lecteur. L'information n'est ni transférée à une base de données, ni stockée. De cette façon, on peut réduire au minimum l'atteinte à la vie privée et protéger les identifiants biométriques de l'employé contre le vol d'identité.

Ne jetons donc pas le bébé avec l'eau du bain, bien que, malheureusement, les eaux de ce bain soient très troubles. La première difficulté à laquelle se heurtent les citoyens qui souhaitent adopter les appareils de surveillance corporelle consiste à reconnaître la logique qui leur est sous-jacente. Dans cette logique, entrent des hypothèses telles que : en raison de sa nature à proprement parler, la surveillance corporelle est plus fiable et donc plus sûre que les autres systèmes ; la mise en place de technologies nous permet d'éviter les enjeux politiques encore plus complexes du profilage racial ; ou la surveillance corporelle est le moyen le plus fiable de détecter les tromperie qui surviennent normalement à la frontière. Cette dernière hypothèse est à la base de technologies comme AVATAR. Par conséquent, nous pouvons opter pour la fouille manuelle faite par un agent plutôt que de choisir le scanneur corporel à l'aéroport. Nous pouvons refuser de nous inscrire à un programme de voyageurs dignes de confiance qui se fonde sur des systèmes biométriques. Nous pouvons contester la décision d'un employeur de faire le suivi des employés au moyen de systèmes biométriques. Nous pouvons aussi faire la queue à la salle de conditionnement physique du quartier pour éviter d'utiliser le mode de paiement biométrique. Malheureusement, le résultat de ces refus de participer n'est souvent guère plus qu'une diminution de notre mobilité – les effets sur le système sont, dans les meilleurs cas, minimes. Alors, comment faire pour se mobiliser plus efficacement face aux enjeux de la surveillance corporelle ?

Il peut se révéler difficile pour le public de participer au débat entourant ces dispositifs puisque les discussions sont dirigées par divers experts

et consultants, dont plusieurs ont des intérêts financiers dans l'industrie qu'ils représentent. Les défenseurs de la biométrie et des scanneurs corporels rejettent la plupart du temps les arguments de ceux qui critiquent ces technologies en soutenant que de telles critiques peuvent compromettent la sécurité nationale. De plus, il se pourrait qu'il n'y ait aucun débat public si les gouvernements ont recours à des stratégies discrètes pour contourner les discussions publiques sur des enjeux qui pourraient soulever la controverse. C'est notamment ce que le gouvernement canadien a fait en signant l'accord Par-delà la frontière en 2011, lequel stipule que le Canada doit partager des données biométriques avec les États-Unis[23].

Le discours souvent impénétrable que tiennent les experts et les technocrates sur ces dispositifs, conjugué aux présumés impératifs de sécurité qui sont associés à leur usage, donnent l'impression que les décisions entourant presque toute les formes de surveillance ont été arrachées au processus démocratique. Or, ce ne devrait pas être le cas. La politique conventionnelle s'applique autant à ce domaine qu'aux autres. Les décisions au sujet des diverses formes de suivi relèvent toujours des politiciens et sont soumises aux comités parlementaires, à l'examen attentif des médias et aux pressions publiques. Bien que les hypothèses influentes sous-jacentes orientent l'application de ces technologies, nous pouvons contester cette logique auprès des personnalités publiques et des organismes de financement. En ayant une solide connaissance de ces appareils et du raisonnement sur lequel ils s'appuient, nous avons toute la latitude nécessaire pour nous inscrire en faux contre leur adoption rapide. Comme des critiques s'élèvent de plus en plus dans la communauté scientifique, on ne saurait trop insister sur la nécessité de profiter de la vague ainsi créée. C'est en notre qualité de citoyen que nous pouvons parler au nom de groupes vulnérables, comme les réfugiés et les demandeurs d'asile qui doivent se soumettre aux technologies de surveillance corporelle les plus avancées et les plus infâmes au Canada et à l'étranger. Nous nous devons de garder un œil critique sur toutes les formes de surveillance corporelle – avant que cet œil ne soit forcé de fournir une empreinte rétinienne.

Notes

1 Voir Simon A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Cambridge, MA, Harvard University Press, 2001) ; Joseph Pugliese. *Biometrics: Bodies, Technologies, Politics* (Londres et New York, Routledge, 2010) ; et Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race and the Technology of Identity* (Durham, NC, Duke University Press, 2011).

2 National Research Council, *Biometric Recognition: Challenges and Opportunities* (Washington, DC, National Academies Press, 2012), p. 5.

3 Voir « Canadian Schools Benefiting from Biometric Payment System », *ID News Canada*, 30 juin 2010, http://www.idsuperstore.ca/idnews/education-id-news/canadian-schools-benefiting-from-biometric-payment-system-19865906/.

4 Pour le système de paiement du parc aquatique, voir « Mon argent au bout du doigt », http://www.calypsopark.com/parc-aquatique/fr/services/mon-argent-au-bout-du-doigt/ ; et « Largest Themed Waterpark in Canada to Open on June 7 », *ID News Canada*, 4 juin 2010, http://www.idsuperstore.ca/idnews/sports-and-recreation-id-news/largest-themed-waterpark-in-canada-to-open-on-june-7-19820328/. Sur le suivi des employés, voir S. Dobson, « Accuracy Vital to Overtime Tracking », *Canadian HR Reporter,* 10 septembre 2007, p. 26, 30 ; D. Harder, « Fingerprint Technology, Pinpoint Accuracy », *Canadian HR Reporter,* 8 septembre 2008, p. 23, 34 ; et « Biometrics Security to Track Working Hours », *The Current, with Anna Maria Tremonti*, CBC Radio 1, 8 novembre 2012, http://www.cbc.ca/thecurrent/episode/2012/11/08/biometrics-security-to-track-working-hours/.

5 Voir « Halifax Port Security to Scan Veins in Hands », *CBC News,* 7 septembre 2007, http://www.cbc.ca/news/canada/nova-scotia/halifax-port-security-to-scan-veins-in-hands-1.665612.

6 Voir Toby Miller, « Surveillance: The Digital Trail of Breadcrumbs », *Culture Unbound* 10, n° 2 (2010), p. 9-14.

7 Voir Reg Whitaker, « Behavioural Profiling in Israel Aviation Security as a Tool for Social Control », dans Elia Zureik, David Lyon et Yasmeen AbuLaban (dir.), *Surveillance and Control in Israel/Palestine: Population, Territory and Power* (Londres et New York, Routledge, 2011), p. 371-385.

8 Voir Jim Bronskill, « Privacy Czar Fears Airport Security Plan Could Involve Racial Profiling », *Globe and Mail*, 9 mars 2012, http://www.theglobeandmail.com/news/politics/privacy-czar-fears-airport-security-plan-could-involve-racial-profiling/article552340/.

9 Sur les systèmes de précontrôle, voir Colin J. Bennett, « What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11 », dans Elia Zureik et Mark B. Salter (dir.), *Global Surveillance and Policing: Borders, Security, Identity* (Cullompton, Royaume-Uni, Willan Publishing, 2005), p. 113-138.

10 Sur le concept de « double de données », voir Kevin D. Haggerty et Richard V. Ericson, « The Surveillant Assemblage », *British Journal of Sociology* 51, n° 4 (2000), p. 605-622.

11 Miller, « Surveillance: The 'Digital Trail of Breadcrumbs », p. 9.

12 Voir Claudia Aradau et Rens van Munster, « Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future », *European Journal of International Relations* 13, n° 1 (2007), p. 89-115.

13 « Biometrics Security to Track Working Hours ».

14 Voir National Research Council, *Biometric Recognition,* p. 4-5 ; et Samuel P. Fenker et Kevin W. Bowyer, « Analysis of Template Aging in Iris Biometrics », document présenté pour le *IEEE Computer Society Biometrics Workshop*, 17 juin 2012, http://www3.nd.edu/~kwb/FenkerBowyerCVPRW_2012.pdf.

15 Voir National Research Council, *Biometric Recognition*, chapitre 4.

16 Voir Benjamin J. Muller, « (Dis)Qualified Bodies: Securitization, Citizenship and Identity Management », dans Peter Nyers (dir.), *Securitizations of Citizenship* (Londres et New York, Routledge, 2009), p. 77-93 ; et Benjamin J. Muller, « Testifying While Critical: Notes on Being an Effective Gadfly », dans Mark B. Salter et Can E. Mutlu (dir.), *Research Methods in Critical Security Studies: An Introduction* (Londres et New York, Routledge, 2012), p. 109-112.

17 Magnet, *When Biometrics Fail,* p. 2.

18 Voir Fenker et Bowyer, « Analysis of Template Aging in Iris Biometrics ».

19 National Research Council, *Biometric Recognition,* p. 5.

20 Fenker et Bowyer, « Analysis of Template Aging in Iris Biometrics ».

21 Voir Aradau et van Munster, « Governing Terrorism Through Risk ».

22 Pour le Canada, voir Meagan Fitzpatrick, « Security Spending After 9/11 Tops $92B », *CBC News*, 7 septembre 2011, http://www.cbc.ca/news/canada/story/2011/09/07/pol-911-security-spending.html ; pour les États-Unis, voir John Mueller et Mark G. Stewart, « Terror, Security, and Money: Balancing the Risks, Benefits and Costs of Homeland Security », document présenté à la convention annuelle de la Midwest Political Science Association, Chicago, 1er avril 2011.

23 Canada, gouvernement, *Plan d'action Par-delà la frontière ; une vision commune de la sécurité du périmètre et de la compétitivité économique*, février 2011, http://actionplan.gc.ca/grfx/psec-scep/pdfs/bap_report-paf_rapport-fra-dec2011.pdf



S’observer les uns, les autres

Du « eux » au « nous »

Lorsque nous pensons à la surveillance, ce sont les activités d’organismes, comme les sociétés ou les services de police qui nous viennent généralement à l’esprit. Ces entités sont en effet des acteurs extrêmement importants dans le domaine de la surveillance. Or, une toute nouvelle sphère de surveillance a fait son apparition : les individus qui s’observent mutuellement sans qu’un organisme coordonne quoi que ce soit. L’ampleur de ce mode de surveillance effectué par les simples citoyens s’est accrue au cours des dernières années ; dans la majorité des cas, cette croissance a été appuyée par les nouvelles technologies de l’information. Voilà une autre grande tendance observée dans la dynamique contemporaine de la surveillance au Canada.

Les gens s’observent entre eux ; ils l’ont toujours fait. Nous nous surveillons mutuellement, parce que cela nous confère un pouvoir stratégique sur les autres, parce que les autres sont fondamentalement intéressants et aussi parce que, tout au long de l’histoire de l’humanité, le fait de s’observer les uns les autres a constitué un avantage du point de vue de l’évolution[1]. Nous apprenons à connaître le monde dans lequel nous vivons, de même que la place que nous y occupons en interagissant avec les autres. Observer et être observé font partie des bases fondamentales à partir desquelles nous définissions qui nous sommes. Nous jouons des rôles (enfant, frère, sœur, parent, employé, ami, époux, amant) et adoptons des caractéristiques en fonction de la manière dont nos performances sont reçues par les autres.

Nous façonnons notre identité en fonction de la façon dont les gens nous perçoivent et réagissent à notre comportement[2].

Bref, les gens ont toujours pratiqué des formes anodines de surveillance au quotidien. Récemment, toutefois, il semble que ce type de surveillance ait pris de l'expansion. Nous nous observons maintenant par des moyens qui, il n'y a pas si longtemps, auraient été impossibles ou tabous. Ce changement s'explique en partie par l'avènement de nouvelles technologies grâce auxquelles il est maintenant facile pour un simple citoyen de devenir un surveillant. Il est également symptomatique d'une culture de surveillance en pleine expansion, dans laquelle la surveillance est devenue un élément courant et banal de la vie sociale.

En général, la surveillance réalisée par les organismes implique souvent que des personnes ayant plus de pouvoir en observent d'autres qui en ont moins. Les policiers surveillent les criminels, les travailleurs sociaux examinent de façon approfondie les bénéficiaires de l'aide sociale et les employeurs surveillent les travailleurs. La surveillance réalisée par les citoyens ordinaires est particulièrement intéressante puisqu'elle peut entraîner la surveillance de personnes appartenant aux classes sociales les plus influentes par des personnes des classes sociales les moins influentes. D'ailleurs, les gens utilisent maintenant des téléphones intelligents munis d'une caméra pour filmer les interventions policières[3]. Les médias du monde mettent également en lumière, parfois de façon exagérée, les manies et les indiscrétions des célébrités et des personnalités politiques.

Ces types de surveillance peuvent toutefois s'immiscer dans des sphères très intimes de notre vie. Prenons par exemple les parents qui ont recours aux nouvelles applications de surveillance pour téléphone intelligent et qui utilisent même des tests antidopage maison pour surveiller leurs enfants. Ils vont même jusqu'à installer des caméras de surveillance dans des articles ménagers (détecteurs de fumée, ours en pluche) pour observer secrètement leur conjoint, leurs enfants et leurs gardiennes. Par ailleurs, les Canadiens qui évoluent dans le vaste monde des réseaux de rencontre en ligne sont également incités à procéder à une vérification officielle des antécédents de leurs prétendants. Plus tard, si la romance tourne au vinaigre, certains retiennent les services de détectives privés qui ont une expertise pour démasquer les époux infidèles.

La forme de surveillance citoyenne la plus intéressante et la plus fluide s'observe sans doute dans le monde des médias sociaux. Compte tenu de l'importance sans cesse grandissante de ces médias, nous nous concentrerons

sur ceux-ci pour démontrer la mesure dans laquelle les citoyens sont de plus en plus pris dans la spirale de la surveillance non seulement en tant que cible, mais également en tant qu'observateur.

La surveillance individuelle : commodité et contact

Comme la surveillance peut avoir des conséquences négatives sur nos relations politiques, sociales et économiques, il peut sembler bizarre de suggérer que la surveillance pourrait aussi être amusante. Il faut admettre toutefois qu'il y a un côté ludique évident à observer les autres et à se faire observer. Cet aspect ludique est particulièrement manifeste dans les sites de réseautage social. Nous publions des photos et des commentaires sur Facebook et Twitter et nous regardons les publications de nos amis, des membres de notre famille et de nos voisins puisque de cette façon nous avons la chance de voir ce qui se passe dans la vie des autres. En publiant des commentaires pour soutenir une cause, des commentaires amusants ou grossiers ou encore en étiquetant des photos ou en « aimant » des produits ou des vidéos, nous modifions également la façon dont les autres nous perçoivent. Bien que ces services puissent être utilisés incorrectement dans les cas par exemple de la traque ou du harcèlement, ils nous aident aussi à renforcer notre sentiment de connexité avec les gens de notre milieu.

Les Canadiens ont adhéré au réseautage social et beaucoup d'entre nous trouvent tout à fait normal d'utiliser les plateformes de médias sociaux. À titre d'exemple, en 2011, quelque 15,4 millions de Canadiens avaient un profil Facebook, plus d'utilisateurs par habitant que tout autre pays[4]. Selon un sondage mené récemment, 79 % des adultes canadiens ont indiqué qu'ils avaient utilisé Facebook dans le dernier mois. Bien que les adultes âgés de moins de 35 ans étaient les plus susceptibles de s'y être connectés (88 %), une majorité importante de personnes âgées de 35 à 54 ans (78 %) et âgées de plus de 55 ans (66 %) étaient également des utilisateurs actifs. Près de la moitié d'entre eux (48 %) ont consacré cinq heures ou plus par semaine aux médias sociaux[5]. Au Canada, les écoles naviguent sur le Web depuis 1999 et, depuis que les jeunes Canadiens ont accès aux médias sociaux, ils ont toujours indiqué en faire usage pour explorer différentes identités, cimenter des amitiés, jouer, s'ouvrir sur le monde et s'exprimer[6]. Pour nombre d'entre nous, le réseautage social fait maintenant partie intégrante de notre vie quotidienne.



Les Canadiens ont adhéré avec enthousiasme à une multitude de médias sociaux (Source : © iStockphoto.com/franckreporter)

Par ailleurs, nous prenons part au réseautage social – observer et être observé – pour aider les autres. Prenons l'exemple d'Hélène Campbell ; cette jeune femme de vingt ans d'Ottawa avait besoin d'une double greffe des poumons. Elle a publié une vidéo sur le Web et a utilisé Twitter pour demander l'aide du chanteur Justin Bieber pour faire la promotion du don d'organe. La vidéo et les gazouillis sont devenus viraux et les membres de la communauté virtuelle ont répondu en grand nombre. La jeune femme a fait le suivi de sa maladie, de sa transplantation et de son rétablissement sur Facebook ; sa page a été vue plus de 600 000 fois par des personnes provenant de 159 pays et un nombre record de nouveaux donneurs d'organe a été enregistré par suite de la campagne de Campbell[7]. Sur des sites comme *Patients Like Me* (des patients comme moi, http://www.patientslikeme.com/), les gens peuvent publier des renseignements sur leurs problèmes médicaux pour que ceux-ci soient regroupés avec ceux des autres et utilisés pour la recherche en santé.

Le partage d'information dans ces cas peut être autant altruiste que productif. Dans le monde virtuel, nous nous observons les uns, les autres. La raison d'être du réseautage social, au-delà du fait d'observer et

d'être observé, est l'impression accrue de connexité que nombre d'entre nous ressentent par rapport au monde qui nous entoure, qui découle en partie de la facilité avec laquelle nous partageons nos vies et nos intérêts avec les autres. Comme nous partageons tant de choses au sujet de notre vie privée avec les gens en ligne, certaines activités nous semblent plus pratiques, comme garder contact avec les amis et la famille, suivre nos émissions et nos vedettes préférées, se divertir selon nos intérêts ou magasiner. Cependant, si une autre personne – un employeur, un policier, un fraudeur, un harceleur, un responsable-marketing ou même un voisin bruyant – outrepasse les limites et nous soumet à une trop grande surveillance, nous avons l'impression que notre intimité a été violée et nous nous sentons plus vulnérables.

Dans le monde virtuel, il n'est pas simple de distinguer la surveillance institutionnelle et de la surveillance individuelle. D'une part, les conséquences peuvent être les mêmes ; tant un policier qu'un conjoint violent peut surveiller le profil d'une personne sur les médias sociaux en vue de contrôler cette personne. Ladite personne verra ce suivi comme une forme de surveillance, peu importe que d'un côté le surveillant soit une institution et de l'autre, un particulier. D'autre part, nous pourrions être enclins à accepter la surveillance faite par une institution qui veut notre bien – les organismes de santé publique surveillent notamment les médias sociaux pour repérer l'éclosion de maladies contagieuses – tandis que nous pourrions ne pas être à l'aise avec le regard attentionné d'un voisin.

Parallèlement, les distinctions entre le suivi fait par les institutions et celui fait par les particuliers peuvent peser dans la balance. Il y a une différence qualitative entre le fait de regarder par curiosité le profil d'une personne dans un média social et la surveillance qu'effectuent les gouvernements et les entreprises au moyen de grandes bases de données et de techniques avancées d'exploration de données, de profilage et d'analyse. Par ailleurs, le suivi fait par les particuliers pourrait bien amplifier la surveillance institutionnelle. Chaque fois que nous publions de l'information personnelle en ligne, nous participons par mégarde à notre propre surveillance puisque cette information est capturée facilement par divers acteurs, des responsables-marketing à l'État en passant par les voleurs d'identité, qui s'en servent à des fins qui leur sont propres[8].

Les lois conçues pour nous protéger du contrôle indésiré reposent principalement sur le consentement : consentons-nous, oui ou non, à ce que l'information que nous générons en utilisant les outils de communication en

réseau soit recueillie, utilisée et divulguée. Les contrats d'utilisation des sites de médias sociaux nous proposent, en petits caractères, d'échanger nos renseignements personnels contre un accès gratuit au site. Toutefois, ce n'est pas parce qu'une personne utilise les médias sociaux qu'elle est encline à laisser tomber sa vie privée. Le « paradoxe de la vie privée » oppose le fait que les gens font état de graves préoccupations au sujet de la protection de leur vie privée, tout en continuant de divulguer des renseignements personnels afin d'obtenir un certain avantage. Ce paradoxe déconcerte toujours les décideurs, pour qui « vie privée » signifie « secret ». En fait, nos attentes relatives à la protection de la vie privée dans les médias sociaux sont beaucoup plus compliquées. Prenons à titre d'exemple certaines des statistiques récentes : 72 % des Canadiens sont d'accord avec l'énoncé suivant : « Lorsqu'une personne publie quelque chose sur un média social, il est légitime qu'une autre personne puisse chercher et voir cette publication ». À l'opposé, presque le même pourcentage (75 %) des gens se préoccupe du fait que d'autres puissent porter atteinte à leur vie privée en voyant leurs renseignements dans les médias sociaux. Enfin, les deux tiers (67 %) disent que, si les gens étaient conscients de ce que l'on peut trouver à leur sujet dans les médias sociaux, ils seraient gênés ou mécontents[9].

Les jeunes et les médias sociaux

Les jeunes Canadiens sont probablement ceux qui sont les plus attentifs aux problèmes de surveillance en ligne. Selon une étude qualitative menée récemment par MediaSmarts, les adolescents canadiens se plaignent de l'intensité élevée de la surveillance effectuée par leurs parents et leurs professeur[10]. Nombre d'entre eux ont intégré les médias sociaux dans leurs communications quotidiennes avec leurs amis. Or, comme les parents sont également nombreux à craindre les échanges en ligne, ils basculent par conséquent dans la surveillance afin de protéger leurs enfants. La plupart des adolescents – et des parents – qui ont pris part à l'étude identifient ce type de surveillance parentale à de l'espionnage ; les enfants se sentent donc comme si on ne pouvait pas leur faire confiance et deviennent méfiants. Une adolescente de Toronto aurait d'ailleurs indiqué que sa mère lui faisait suffisamment confiance pour qu'elle amène un garçon à la maison, mais ne lui faisait pas suffisamment confiance pour qu'elle soit amie avec lui sur Facebook. Elle a ajouté qu'elle trouvait la situation déprimante[11].

Avec cette surveillance des parents, il est difficile pour les adolescents de combler leurs besoins développementaux au moyen des réseaux sociaux, c'est-à-dire se dissocier de la famille, s'épanouir et assumer des responsabilités d'adulte. Pour y arriver, les adolescents ont besoin que l'on respecte leur vie privée et qu'on leur fasse confiance. Citons en exemple un autre adolescent de Toronto qui affirmait qu'à un certain point, les parents devraient les laisser tranquilles et accepter de ne pas tout savoir sur eux[12].

Il est important de noter que les adolescents qui ne sont pas surveillés d'office par leurs parents se sentaient plus à l'aise d'aller les voir s'ils ont un problème de harcèlement en ligne ou s'ils jugent un contenu en ligne offensant. Ironiquement, l'utilisation des médias sociaux par les enfants fait craindre aux parents que des observateurs secrets s'en prennent à leurs enfants ; par conséquent, pour les protéger de ces inconnus, les parents se mettent à surveiller leurs enfants. Néanmoins, il se peut que cette surveillance finisse par miner la confiance qui est au cœur de la relation entre le parent et l'enfant. Le côté ludique de la visibilité électronique devient alors étroitement lié à des inquiétudes et à une marque nuisible d'attention.

Les jeunes Canadiens ayant participé à l'étude de MediaSmarts soutenaient par ailleurs qu'ils étaient conscients que leurs amis et leurs pairs les observent. Ils ont donc recours à une série de règles sociales pour les aider à orienter leur couverture personnelle en ligne. D'ailleurs, il existe des tabous bien ancrés, surtout pour les filles, au sujet de la publication de photos gênantes de leurs amis. Lorsqu'une personne publie des commentaires méchants à propos d'un ami, les jeunes tentent de publier des choses positives au sujet de cet ami afin de tenter de rétablir sa réputation en ligne. Ils appliquent également certaines stratégies pour protéger leur vie privée ; ils peuvent notamment publier uniquement des paroles de chanson ou des citations que seuls les initiés peuvent comprendre ou ils créent plus d'un compte Facebook afin de restreindre ce que les membres de leur famille peuvent voir. Par conséquent, on constate l'émergence d'une série de règles sociales dans ces groupes qui aident à contrôler la visibilité des jeunes en ligne et qui observe qui.

Or, ces jeunes Canadiens reconnaissent que l'information publiée en ligne est perméable et que, peu importe ce qu'ils font, les autres peuvent le voir même s'ils activent les paramètres de sécurité les plus élevés. L'information publiée à l'intention d'un public (amis ou famille) peut parfois être vue par d'autres gens, ce qui peut entraîner des conséquences fortuites. Citons par exemple les individus malveillants comme les voleurs d'identité

Un véritable jeu d'enfant !

Dès les premiers balbutiements du Web, les spécialistes du marketing et les organismes ont rivalisé pour obtenir l'attention des jeunes internautes, les enfants. Webkinz, entreprise appartenant à la firme de jouets Gantz et exploitée par celle-ci, encourage les enfants à consulter fréquemment son site Web en rendant leur animal virtuel malade s'ils ne le visitent pas assez souvent. Dès que l'enfant revient sur le site, il est accueilli par un animal avec la mine basse et avec une bouillotte sur la tête. On signale alors à l'enfant que son animal s'est ennuyé pendant son absence et que pour qu'il retrouve sa joie il doit le visiter tous les jours et cliquez sur le bouton « I love Webkinz »[1].

Les sites comme Webkinz encouragent généralement les enfants à intégrer la marque dans les activités dans le monde réel. On demande aux enfants d'envoyer leurs illustrations et anecdotes et d'organiser des fêtes en y intégrant des éléments trouvés sur le site de la marque. Une version antérieure de la poupée Barbie en ligne pouvait même téléphoner aux enfants pour leur lire une histoire avant qu'ils se couchent.

La surveillance intégrée aux sites de jeu pour enfants est présentée comme une façon de protéger les enfants des cyberprédateurs. On dit aux parents que les sites sont surveillés pour

et les cambrioleurs, qui fouillent les médias sociaux pour dénicher des renseignements personnels qui pourraient être utiles pour commettre une fraude ou pour repérer les maisons des gens partis en vacances. Toutefois, ce sont les organismes qui recueillent nos données à leurs propres fins qui sont maintenant légion.

Surveillance institutionnelle par les médias sociaux

Parfois, le processus est transparent. La visibilité qui accompagne la participation au monde virtuel favorise l'utilisation de l'information publiée à d'autres fins. Les photos, les vidéos et les commentaires publiés dans un contexte peuvent être utilisés dans un autre en vue de demander aux gens de rendre des comptes sur leurs comportements dans leur vie privée. Il est arrivé à de rares occasions qu'un employeur qui souhaitait recruter des employés demande aux candidats potentiels leur mot de passe Facebook pour voir tout ce qui a été publié sur le profil avant de prendre une décision. Ces situations

s'assurer que les enfants sont en sécurité et que les flots d'information sont recueillis pour améliorer l'expérience virtuelle des enfants.

Club Penguin est un autre site initialement créé par des Canadiens, mais qui a depuis été acheté par Disney. Ce site encourage ses utilisateurs à s'inscrire pour espionner d'autres enfants. À titre de membre de la « Penguin Secret Agency » (P.S.A.), l'enfant reçoit un téléphone spécial d'espion et le F.I.S.H. (Factual Informative Spy Handbook). À titre de membre, il a également accès au quartier général où il est informé que sa « mission » est de signaler tous les pingouins qui seraient méchants ou impolis, qui utilisent des gros mots, qui demandent ou révèlent des renseignements personnels à d'autres enfants ou qui enfreignent les règles du site. Les enfants qui parviennent à dissimuler leur identité d'espion et qui sont de bons espions reçoivent des récompenses virtuelles. De cette façon, les enfants apprennent que la surveillance est amusante et utile et ils apprennent à socialiser dans une culture de surveillance. Les subtilités juridiques du site stipulent toutefois que l'information divulguée par les enfants lorsqu'ils naviguent sur le site, y compris tout bricolage, illustration, anecdote ou autre matériel original, devient la propriété de l'entreprise.

1. Selon une étude menée en 2009. Voir aussi Gary T. Marx et Valerie Steeves, « From the Beginning: Children as Subjects and Agents of Surveillance », *Surveillance and Society* 7, no 3 (2010), p. 6-45.

ont toutes soulevé la controverse. De plus, plusieurs professionnels, y compris des professeurs, ont été punis ou renvoyés pour des publications dans les médias sociaux. Ces situations nous rappellent que la ligne est bien mince entre s'amuser à s'exposer publiquement et devenir la cible de formes conventionnelles de surveillance hiérarchique.

En règle générale, le flux d'information est toutefois dissimulé et nous ne savons pas comment notre information est utilisée pour influer nos expériences et restreindre nos possibilités. Sur cette question, les statistiques peuvent aussi en dire long. En effet, 80 % des Canadiens interrogés estiment qu'ils ont leur mot à dire quant au traitement réservé à leurs renseignements personnels. De plus, la vaste majorité s'oppose à ce que les entreprises puissent parcourir leurs courriels pour obtenir de l'information au sujet de leurs intérêts (96 %), faire le suivi du contenu consulté sur le Web (88 %), communiquer de l'information au sujet des sites Web qu'ils consultent (90 %) ou divulguer l'information qu'ils publient dans les médias sociaux (90 %)[13]. Or, toutes ces pratiques sont communes et sont motivées par un modèle d'affaires qui tire profit de l'information que nous révélons

en menant notre vie en ligne[14]. Dans ce modèle, des technologies d'exploration de données servent à séparer les gens en catégories afin que l'on puisse leur offrir des services des publicités taillées sur mesure selon leur profil. Les détails de ces pratiques sont plus ou moins explicites dans le libellé des accords d'utilisation et dans les politiques de protection des renseignements personnels, mais ces documents sont systématiquement critiqués pour leur manque de clarté.

La visibilité tous azimuts que produisent les médias sociaux est le résultat direct du fonctionnement des algorithmes qui servent à catégoriser les individus selon une logique marchande. En utilisant Facebook, Instagram, Pinterest et d'autres médias sociaux, nous contribuons à la classification faite par les organismes qui utilisent nos données. Nous publions nos préférences, nos habitudes, nos goûts musicaux et alimentaires, nos opinions politiques ou nos convictions religieuses ; toutes ces publications servent à nous placer dans une catégorie. L'ajustement des paramètres de protection des renseignements personnels n'empêchera pas les tiers de nous évaluer et de nous juger. En effet, les corporations peuvent en apprendre beaucoup sur nous simplement en regardant les amis qui ont un lien virtuel avec nous.

La plupart des gens croient que ces renseignements ne servent qu'à déterminer les publicités qui nous seront destinées quand nous naviguons dans Internet. Il est intéressant à plusieurs égards de constater à quel point la publicité est maintenant intégrée à notre univers social. Bien que la majorité des gens supposent (à tort) qu'ils sont immunisés contre l'influence des publicités, en réalité la publicité a des effets considérables sur nos relations, notre conception de ce qu'est une bonne vie et sur le type de personne que nous souhaiterions être. Elle ne constitue toutefois que la pointe de l'iceberg. Les entreprises utilisent l'information qu'elles recueillent sur nous pour construire notre environnement social à proprement parler. Elles souhaitent ainsi promouvoir certains types d'identités et de relations qui font progresser leurs intérêts commerciaux. Par exemple, les responsables des espaces de jeux en ligne glanent des données personnelles sur les enfants et s'en servent pour incorporer la marque à leur identité. Les sites qui utilisent les médias sociaux pour vendre des tampons et qui offrent des « conseils » aux adolescentes et qui les encouragent à parler à l'entreprise si elles ne peuvent plus le faire avec leur mère comme lorsqu'elles étaient enfants. Facebook suggère également à ses utilisateurs d'ajouter certains produits à la liste des choses qu'ils « aiment » afin d'exprimer leur individualité. En somme, toutes

ces pratiques façonnent le type de personne que nous sommes et y imposent des contraintes, et ce, sans même que nous le sachions.

Par ailleurs, les médias sociaux n'offrent pas toujours l'image de nous que nous préférons ; les catégories dans lesquelles nous entrons ne correspondent pas nécessairement à la manière dont nous nous percevons. Ce phénomène est surtout problématique pour les gens qui sont marginalisés d'une quelconque façon. D'ailleurs, le profilage est utilisé pour déterminer quel groupe de gens est le plus susceptible de dépenser le plus pour certains biens. À Ottawa, des magasins de meubles, d'électroniques et d'articles ménagers ont même quitté des quartiers pauvres, parce que les gens qui y vivent n'entrent pas dans la catégorie démographique de la clientèle recherchée. Par conséquent, les laissés-pour-compte doivent maintenant prendre le transport en commun pour se rendre à un magasin déménagé plus loin et y acheter des aliments. De plus, les cadeaux offerts aux personnes qui correspondent aux profils d'un consommateur désirable dépendent d'un système qui offre moins aux personnes qui sont considérées comme plus vulnérables.

Il en va de même pour ceux d'entre nous qui captent l'attention des autorités. En effet, grâce aux médias sociaux, les gouvernements peuvent plus facilement identifier et suivre les personnes qui touchent des prestations d'assurance-emploi ou d'aide sociale ou encore qui participent à des activités de dissidence politique. La norme qui régit habituellement la surveillance de l'État, soit les motifs raisonnables et probables de soupçonner qu'une infraction a été commise, est esquivée lorsque les organes de contrôle n'ont qu'à aller sur Internet pour observer les citoyens. Paradoxalement, les lois sur la protection des renseignements ont accru encore plus le recours à cette pratique en permettant à des sociétés comme Facebook ou Google de divulguer des renseignements personnels aux policiers et aux services de renseignements. Dans le cadre d'une enquête sur l'application de toute loi fédérale, provinciale ou municipales ou d'un pays étranger, ces organes n'ont qu'à demander ces renseignements aux sociétés ; ils n'ont pas à obtenir un mandat. Voilà un seuil légal très peu élevé pour des capacités de surveillance si vastes.

Ce genre de pratiques donne lieu à de sérieuses préoccupations au sujet de la relation démocratique entre le citoyen et l'État. Les dispositions législatives sur l'accès à l'information et sur la protection des renseignements personnels ont été adoptées dans les années 1970. Elles avaient pour objectif d'assurer la transparence de l'État envers les citoyens et de faire

Les médias sociaux et les émeutes de 2011 à Vancouver

Les gens se tournent vers les médias sociaux pour rester connectés. Cependant, les médias sociaux peuvent également servir à exercer une forme populiste de justice criminelle. En effet, des sites comme Facebook permettent un nouveau type de surveillance, où la visibilité peut devenir une punition au moyen de la dénonciation et de la condamnation publique.

Le 15 juin 2011, les Canucks de Vancouver ont perdu la finale de la Coupe Stanley contre les Bruins de Boston. Après cette déception, près de 100 000 personnes ont manifesté violemment dans les rues de Vancouver. Les manifestants ont incendié des voitures, pillé des vitrines de magasins et agressé les passants. Bien que des émeutes relatives au hockey se soient déjà produites dans le passé, l'opinion publique en a toujours eu une faible estime. Or, auparavant, les participants à ces émeutes échappaient à l'examen public. Comme pour beaucoup d'autres sphères de la vie sociale, l'omniprésence des appareils mobiles et des plateformes de réseautage social est venue changer le type de visibilité à laquelle s'exposaient les participants aux émeutes.

Presque dès le début de l'émeute à Vancouver, les gens se sont tournés vers Facebook pour exprimer leur indignation. On a vu apparaître des groupes sur le sujet; un de ces groupes, le « Vancouver Riot Pics: Post Your Photos » (photos de l'émeute de Vancouver : publiez vos photos), a attiré plus de 100 000 membres, plus de 5 millions de visites et la publication d'innombrables photos en cinq jours. Le contenu provenait de plusieurs sources, notamment des appareils photo des utilisateurs, d'arrêts sur image et des policiers. Or, des images ont également été glanées sur les profils des suspects. Bien qu'on puisse douter de la recevabilité juridique de ces « preuves », ce type de groupe marque un tournant vers une plus grande présence policière dans la vie sociale dans les médias sociaux et les technologies mobiles. Les utilisateurs ont

en sorte que l'État rende des comptes aux citoyens. Quant au citoyen, il se voyait accorder une certaine intimité par l'État puisque c'est cette intimité qui lui assure son autonomie. De nos jours, toutefois, il est de plus en plus facile pour l'État d'avoir accès à l'information sur la vie privée des citoyens. Citons comme exemple l'Albertain qui a été accusé de voies de fait après avoir publié sur Facebook [traduction] « Moi, superman, j'ai frappé un gars ». Lorsqu'il a comparu devant le tribunal, il a affirmé qu'il n'avait pas frappé la victime ; le juge ne l'a pas cru en raison du commentaire formulé en ligne

fourni directement des photographies, des noms et leur version des événements. Ils ont également dirigé leur colère vers des cibles visibles. Les personnes soupçonnées d'avoir participé aux émeutes ont été mêlées à une véritable chasse aux sorcières virtuelle et bon nombre ont été stigmatisées par la suite. Camille Cacnio, étudiante dans une université locale, a été filmée alors qu'elle pillait un magasin de vêtement. Elle a été identifiée publiquement, ce qui a entraîné la prise de mesures juridiques normales, mais ce qui l'a aussi offerte sur un plateau à la Ville qui était à la recherche d'un bouc émissaire. Cacnio est par la suite devenue la cible de propos haineux, qui pour la plupart étaient racistes et sexistes. La campagne de haine s'est propagée dans Internet et a eu des répercussions immédiates sur sa qualité de vie. Elle a été renvoyée de son travail et demeurera à jamais visible sur Internet pour ce qui sera sûrement l'événement le plus honteux de toute sa vie.

Bien que les participants aux émeutes doivent répondre de leurs actes, la façon dont ils ont été pourchassés et calomniés sur les médias sociaux témoigne de la montée d'une forme perturbante de vigilantisme en ligne. L'hystérie collective qui a alimenté les émeutes a eu son pendant sur Internet. Tout le tort causé par la surveillance, y compris le profilage, les préjudices et le frein qu'elle impose aux possibilités dans la vie, a été en réalité rendu à la foule. Cette foule électronique n'était pas assujettie à des normes professionnelles. Bien que les utilisateurs aient pu penser aider les policiers, dans les faits, une telle foule peut être un fardeau pour les policiers, car ses interventions peuvent causer davantage de tort social (les suspects ont reçu des menaces, des familles ont dû déménager, etc.). Les policiers mettent actuellement à l'essai des techniques et des technologies pour vérifier le contenu dans les médias sociaux, dont des renseignements de source ouverte, l'interception légale et le piratage psychologique (*social engineering*). On est en droit de se demander quel sera le type de surveillance utilisé la prochaine fois que les amateurs de hockey descendront dans la rue.

(*R.* c. *Tscherkassow*, 2010 ABPC 324). Dans une autre affaire, trois adolescents de la Colombie-Britannique ont été suspendus de l'école après avoir été impliqués dans une bagarre qui a été filmée puis publiée sur YouTube, et ce, même si la bagarre a eu lieu entre des adversaires consentants et qu'aucune accusation criminelle n'a été déposée. L'adolescent qui a affiché la vidéo a aussi été menacé de suspension[15]. Dans ces deux cas, il était peu probable que des sanctions officielles soient imposées pour ce genre d'actes, mais ce sont les médias sociaux qui ont attiré l'attention des autorités sur les incidents.

L’agent Bulles

> *[Traduction] Si les bulles me touchent, vous serez arrêtée pour voies de fait.*
> —Agent Bulles du service de police du Grand Toronto

Il est difficile de croire que ce genre de déclarations puisse être faite par un agent du service de police de Toronto. Et pourtant, une recherche rapide sur YouTube avec les mots clés « Officer Bubbles » (agent Bulles) vous permettra de trouver une vidéo dans laquelle vous verrez un agent de police prononcer avec assurance ces paroles avant d’arrêter une femme pour avoir soufflé des bulles sur lui. Au dire de l’agent Bulles, dont le vrai nom est Adam Josephs, souffler des bulles équivaut à des voies de fait puisque le « détergent » utilisé pour faire des bulles peut causer des blessures s’il entre en contact avec les yeux.

L’agent Bulles est devenu célèbre sur Internet après qu’une vidéo de l’arrestation de Courtney Winkels, la souffleuse de bulles, eut été publiée. La vidéo originale a été vue plus de 900 000 fois et a été montrée par plusieurs médias nationaux et internationaux. Cette vidéo a également alimenté l’imaginaire de certains internautes qui ont produit une série de dessins animés dans laquelle on peut voir l’agent Josephs arrêter le père Noël et Barack Obama.

Le cas de l’agent Bulles n’est qu’un exemple des drôles d’interventions de maintien de l’ordre qui ont été rendues publiques par les citoyens au moyen de leur caméra. Cet incident porte à croire que, bien que les policiers aient toujours été très visibles comme représentants

Parallèlement, les processus dont se sert le gouvernement pour recueillir de l’information au sujet des citoyens sont appliqués derrière des portes closes. Autrement dit, aucun contrôle judiciaire n’est effectué lors de l’exploration de données, de l’établissement de correspondances et de l’application d’algorithmes pour déterminer les risques. On assiste donc à un renversement des positions : l’État qui autrefois était transparent devient opaque et les citoyens qui avaient une vie privée deviennent transparents. Qui plus est, ce phénomène menace de perturber l’équilibre démocratique.

Cependant, la visibilité est une arme à double tranchant. En effet, les médias sociaux ont joué un rôle pour forcer l’État à rendre des comptes concernant des abus de pouvoir. La vidéo de la fouille à nu de Stacy Bonds par des policiers d’Ottawa et celle d’un policier poussant par terre une femme handicapée dans le quartier Downtown Eastside de Vancouver sont devenues

en uniforme du système juridique, les citoyens et les militants ont pu accroître considérablement leur visibilité puisque les caméras sont devenues très abordables et accessibles au cours des dix dernières années. Grâce aux caméras portatives, les citoyens peuvent consigner les interventions de policiers comme l'agent Josephs et braquer les projecteurs sur leurs comportements douteux au moyen des médias sociaux.

De plus, les caméras et les médias sociaux permettent au public d'examiner et de critiquer le comportement des policiers et de faire état de leurs préoccupations aux institutions policières. Par conséquent, les policiers sont maintenant soumis à ce nouveau régime de surveillance qui encourage le débat public au sujet des incidents impliquant la police et à une nouvelle forme d'évaluation du rendement. Cependant, l'incidence politique de ces nouveaux régimes de surveillance est ambiguë et complexe. Ces régimes suscitent des questions comme : cette surveillance entravera-t-elle la capacité des policiers de servir l'intérêt public? La capacité du public de surveiller les policiers permettra-t-elle de détecter les pratiques atypiques? Malheureusement, il n'y a pas de réponses simples à ces questions puisque l'incidence de cette nouvelle visibilité des policiers est ambiguë et nécessite une recherche approfondie. Cela dit, force est de constater que cette nouvelle visibilité a rendu accessible une quantité d'information sans précédent au sujet des policiers et crée de nouveaux défis pour les services de police pour ce qui est de maintenir leur image publique[1].

1. Andrew John Goldsmith, « Policing's New Visibility », *British Journal of Criminology* 50, no 5 (2010), p. 914-934.

virales sur YouTube et ont contribué à mobiliser des citoyens qui ont exprimé leurs préoccupations et exigé des justifications[16]. Enfin, les images prises au moyen de téléphones cellulaires des policiers en action lors des manifestations en marge du G20 à Toronto ont aidé à placer la question des abus de pouvoir à l'avant-scène du débat sur la mondialisation[17].

En raison des rapports complexes que nous entretenons avec la surveillance, il est à la fois plus facile et plus difficile d'exiger des comptes des institutions influentes. Nous pouvons certes nous attendre à avoir encore plus de mal à déterminer qui contrôlera le produit de toute cette surveillance dans l'avenir. D'ailleurs, dans certains États américains, il est maintenant interdit de filmer les policiers. De plus, Apple a fait breveter récemment un appareil qui permettrait aux policiers de désactiver la fonction d'enregistrement sur les appareils mobiles dans une zone définie. Toutefois, il se peut

que l'abandon des médias sociaux ne soit plus une option. Si nous refusons de dévoiler des éléments personnels, non seulement nous aurons plus de mal à savoir quand des activités ont lieu ou à participer au débat public sur l'enjeu du jour, mais nous aurons également du mal à faire des achats, à obtenir un prêt bancaire ou à obtenir un emploi.

Conclusion

Par conséquent, sur le plan de la surveillance, les médias sociaux ont au moins deux facettes. Nous utilisons les technologies en réseau pour observer nos amis, nos voisins et les membres de notre famille et nous leur permettons ainsi de nous observer. Il devient ainsi plus difficile de faire une distinction entre le flot social d'information dans une communauté et l'instrumentalisation de cette information par les gouvernements, les employeurs et les entreprises. Bien que nous soyons peu à accumuler des quantités astronomiques de données sur les autres, nous contribuons tous à ces bases de données en publiant en ligne des détails sur notre vie privée et sur celle des autres.

Reste que les médias sociaux demeureront probablement un moyen de se connecter, de partager et de garder contact. Ils nous aideront également à veiller sur les autres et à en prendre soin dans un monde qui deviendra de plus en plus fragmenté et anonyme. Beaucoup d'histoires comme celle d'Hélène Campbell d'Ottawa circulent au sujet de personnes qui ont été victimes d'un accident ou qui souffrent d'une maladie et qui ont été aidées par des amis éloignés grâce aux médias sociaux. De nouvelles questions sont toutefois soulevées sur ce moyen d'observation et sur les conséquences de la surveillance dans les médias sociaux.

Ainsi, le défi dépasse le simple fait de savoir qui vous observe, pourquoi ils le font ou quelles en seront les conséquences. Si la surveillance s'inscrit dans un contexte qui est considéré comme « amusant », non seulement elle rend inoffensif ce que certains pourraient percevoir comme le contraire, mais elle contribue également à apprivoiser la surveillance et à la rendre plus normale et plus naturelle[18]. Même si les autres peuvent être gênés ou blessés s'ils apprenaient que nous les observons, nous continuons tout de même de le faire. Nous n'hésitons pas à nous engager dorénavant dans le même type d'activités que les gouvernements ou les sociétés et ces activités présentent toujours un risque de préjudice. Le sens profond de l'appel à être le

gardien de nos frères et sœurs doit être revu dans cette ère numérique. Dans un monde où nous observons couramment les autres et où nous savons que les autres nous observent en retour, nous devons nous demander si nous surveillons *les autres* ou si nous surveillons *pour les autres*.

Notes

1 John L. Locke, *Eavesdropping: An Intimate History* (Oxford, Oxford University Press, 2010).

2 Voir Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven, Yale University Press, 2012) ; Daniel J. Solove, *Understanding Privacy* (Cambridge, MA, Harvard University Press, 2008) ; et Valerie Steeves, « Reclaiming the Social Value of Privacy », dans Ian Kerr, Valerie Steeves et Carole Lucock (dir.), *Privacy, Identity and Anonymity in a Networked World: Lessons from the Identity Trail* (New York, Oxford University Press, 2009), p. 191-208.

3 Andrew John Goldsmith, « Policing's New Visibility », *British Journal of Criminology* 50, nº 5 (2010), p. 914-934.

4 Michael Oliveira, « Canada 'Most Socially Networked' Title Slipping Away », *Globe and Mail,* 29 février 2012, http://www.theglobeandmail.com/technology/digital-culture/social-web/canadas-most-socially-networked-title-slipping-away/article550205/.

5 David Lyon et Emily Smith, « Surveillance, Social Media and Participation: Being Watched and Watching », ouvrage en cours de rédaction, Centre des études sur la surveillance, Université Queen's, Kingston, ON.

6 Valerie Steeves, *Jeunes Canadiens dans un monde branché, Phase II : Tendances et recommandations,* Ottawa, MediaSmarts, 2005 ; et *Jeunes Canadiens dans un monde branché, Phase III : Discuter de la vie en ligne entre parents et jeunes,* Ottawa, MediaSmarts, 2012, http://habilomedias.ca/recherche-et-politique.

7 Barbara Turnbull, « Ottawa's Hélène Campbell Dreaming of Future, and More Transplant Donors », *Toronto Star,* 3 juin 2012, http://www.thestar.com/life/2012/06/03/ottawas_hlne_campbell_dreaming_of_future_and_more_transplant_donors.html.

8 Voir Daniel Trottier, *Social Media as Surveillance: Rethinking Visibility in a Networked World* (Londres, Ashgate, 2012) ; et John Cheney-Lippold, « A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control », *Theory, Culture and Society* 28, nº 6 (2011), p. 164-181.

9 Lyon et Smith, « Surveillance, Social Media and Participation ».

10 Valerie Steeves, *Jeunes Canadiens dans un monde branché, Phase III : Discuter de la vie en ligne entre parents et jeunes*, p. 16-24.

11 Ibid., p. 19.

12 Ibid., p. 18.

13 Lyon et Smith, « Surveillance, Social Media and Participation ».

14 Voir Mark Andrejevic, « The Kinder, Gentler Gaze of Big Brother: Reality TV in the Era of Digital Capitalism », *New Media and Society* 4, nº 2 (2002), p. 251-270 ; Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence, University Press of Kansas, 2007) ; Mark Andrejevic, « Exploitation in the Data Mine », dans Christian Fuchs, Kees Boersma, Anders Albrechtslund et Marisol Sandoval (dir.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (Londres et New York, Routledge, 2012, p. 71-88) ; et Nicole S. Cohen, « The Valorization of

Surveillance: Towards a Political Economy of Facebook », *Democratic Communiqué* 22, nº 1 (2008), p. 5-22.

15 Jason Hewlett, « School District Investigates YouTube Fight Video », *Daily News*, Kamloops, 9 juin 2011, http://www.kamloopsnews.ca/article/20110609/KAMLOOPS0101/306099985/-1/kamloops/.

16 « Stacy Bonds Police Video », https://www.youtube.com/watch?v=P71BvVCbFXk ; « CCTV: Vancouver Police Shoving Down 90 Pound Woman with Multiple Sclerosis in Downtown Eastside », https://www.youtube.com/watch?v=n8K7j5olaeg.

17 « Adam Nobody Gets Beat Up by Police », https://www.youtube.com/watch?v=NI2b8igEYc8.

18 Voir Ariane Ellerbrok, « Playful Biometrics: Controversial Technologies Through the Lens of Play », *Sociological Quarterly* 52, nº 4 (2011), p. 528-547.

Conclusion
Alors, que pouvons-nous faire ?

Nous pourrions conclure en disant que les diverses tendances exposées dans cet ouvrage sont simplement inarrêtables, et c'est ce que croient certains. C'est parfois le message que véhiculent clairement les personnes et les organismes qui ont un intérêt direct puisqu'ils ont recours à ces technologies pour traiter de plus en plus de données personnelles en vue de réaliser des profits. On croit entendre l'écho des propos tenus par Scott McNealy de Sun Microsystems il y a une dizaine d'années : de toute façon, la vie privée n'existe pas et il faudra s'y faire[1].

Comme nous le montrent les neuf tendances que nous venons d'analyser, ce conseil est simpliste et biaisé. Les données personnelles utilisées par divers organismes permettent de parvenir à différents résultats, que ce soit pour le meilleur, ou pour le pire. Cependant, en règle générale, le pouvoir organisationnel sur les individus est renforcé par la plupart des pratiques de surveillance. Selon les grands axes de cet ouvrage, nombre de pratiques pourraient maintenant être appelées de la surveillance ; la surveillance ne s'entend plus seulement des policiers qui font de l'écoute téléphonique ou de la filature. En rejetant la vie privée, McNealy tire une conclusion simpliste et omet de tenir compte de tout l'éventail des pratiques de surveillance. De plus, il émet une opinion biaisée en tentant de détourner l'attention du pouvoir réel de ces pratiques dans la vie quotidienne de la population.

Nous ne sommes donc pas du même avis que McNealy. Pour toutes les pressions exercées en faveur de l'expansion de la surveillance, il existe une force importante de défense de la vie privée qui pousse dans l'autre direction. Heureusement, au Canada, nous nous sommes déjà dotés d'outils pour résister aux conséquences négatives de ces tendances et pour affirmer et réaffirmer le simple principe suivant : les données personnelles ne sont pas une ressource gratuite que les organismes privés et publics peuvent exploiter comme bon leur semble. Nos vies sont devenues plus transparentes en raison de cette surveillance accrue. Nous devons donc entreprendre des initiatives qui seront axées sur les gens ordinaires dans la vie de tous les jours et qui viseront à accroître la transparence des pratiques de surveillance, surtout de celles qui sont intégrées aux transactions, aux dispositifs et aux cadres qui nous sont familiers.

Ces initiatives requerront toutefois des actions sur plusieurs fronts. Nous ne pourrons freiner la surveillance qu'en adoptant de multiples approches : loi, autoréglementation, éducation, protections technologiques, sans oublier les traditionnelles pressions politiques. Dans certains contextes, il est démontré que les organismes peuvent être forcés de mettre un frein à l'accumulation et au traitement abusif de l'information dont a fait état cet ouvrage, et parfois de faire marche arrière.

Le point de départ le plus évident est la loi.

La vie privée jouit de certaines protections constitutionnelles. En effet, on peut lire à l'article 8 de la *Charte canadienne des droits et libertés* : « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Selon l'interprétation qu'en ont faite les tribunaux, les policiers doivent généralement obtenir un mandat avant de pouvoir surveiller un citoyen. Par conséquent, chaque fois que des policiers font une fouille sans avoir de mandat, il incombe à l'État de prouver que la fouille n'a pas enfreint le droit de l'individu de s'attendre raisonnablement à ce que sa vie privée soit protégée. Si les policiers ne peuvent le prouver, le tribunal rejettera généralement les preuves obtenues lors de cette fouille.

Toutefois, lorsqu'il s'agit d'appliquer l'article 8, les difficultés surgissent des menus détails. La Cour suprême du Canada tend à diviser la vie privée en catégories distinctes, mais tout de même interreliées : les aspects qui ont trait à la personne, aux lieux et à l'information. La vie privée qui a trait à la personne bénéficie de la plus forte protection « parce qu'elle protège l'intégrité corporelle et plus particulièrement le droit de refuser toute palpation ou exploration corporelle qui dévoilerait des objets ou des matières qu'une

personne veut dissimuler »[2]. Une moins grande protection est conférée aux aspects qui ont trait aux lieux selon l'endroit où l'on se trouve. Les tribunaux sont surtout soucieux de protéger la vie privée à l'intérieur des maisons. Cependant, dès que vous passez la porte de votre maison, les protections s'affaiblissent.

Les aspects qui ont trait à l'information tendent à se trouver au bas de l'échelle et à mériter les protections les plus faibles. Néanmoins, la Cour suprême a reconnu que les citoyens ont un droit à la vie privée en ce qui concerne l'information « tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu »[3]. La protection de la vie privée dans ce cas se fonde sur [traduction] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués »[4].

L'un des problèmes est que les nouvelles technologies sont venues brouiller les distinctions entre les aspects ayant trait à la personne, aux lieux et à l'information de la vie privée. Lorsque les corps et les lieux peuvent être transformés en information, le niveau de protection est souvent réduit au plus petit dénominateur commun. D'ailleurs, bien que les policiers ne puissent procéder à des tests physiques envahissants sans avoir obtenu de mandat, ils peuvent analyser l'ADN contenu dans un mouchoir souillé qu'aurait jeté un suspect pendant l'interrogatoire. De la même façon, bien que les policiers ne puissent entrer dans une maison et procéder à une perquisition de drogue sans un mandat, ils peuvent vérifier les factures d'électricité d'une maison pour voir si les occupants utilisent suffisamment d'électricité pour opérer une installation de culture de la marihuana.

Comme l'information peut maintenant être révélée par notre corps, notre emplacement et nos appareils électroniques, les tribunaux ont plus de mal à circonscrire ce qu'est une attente raisonnable de protection de la vie privée. D'ailleurs, dans l'affaire *R.* c. *Tessling,* la GRC a eu recours à un avion muni d'un appareil photo qui utilise un système infrarouge à vision frontale (« FLIR ») pour survoler la propriété de l'accusé où il exploitait une installation de culture de la marihuana. L'image ainsi prise devait servir à détecter les fuites de chaleur. La Cour suprême a indiqué que cette façon de faire était permise par la *Constitution* en vertu de l'article 8 de la *Charte* puisque les aspects du droit à la vie privée ayant trait à l'information donnent lieu à des protections inférieures à celles accordées au droit à la vie privée ayant trait aux lieux. Par ailleurs, dans l'affaire *R.* c. *A.M.*, la Cour suprême

a conclu que les odeurs provenant des vêtements ou des effets personnels qui sont détectées par un chien renifleur constituent un renseignement à l'égard duquel l'accusé doit avoir une attente raisonnable en matière de vie privée[5]. Bien entendu, les actions en justice ne sont pas le seul moyen de contester les atteintes à la vie privée. Prenons par exemple l'opposition soulevée par les compteurs intelligents, qui permettent une transmission bidirectionnelle entre le compteur électrique d'une maison et le fournisseur d'électricité[6]. L'adoption de ces compteurs a entraîné la formation d'une coalition de citoyens très active au Canada. Nous examinerons ce type de réactions un peu plus loin.

Contester la surveillance en invoquant l'article 8 de la *Charte* peut donc mener à des résultats ambigus. Ces contestations peuvent également prendre du temps et coûter très cher. Les protections de la vie privée imposées par la loi seraient donc plus pertinentes pour le citoyen ordinaire. Au cours des vingt dernières années, une mosaïque complexe de textes législatifs a été créée en vue de réglementer les pratiques de surveillance et de protéger la vie privée. À la différence d'autres pays, le régime juridique de protection de la vie privée du Canada se divise généralement en deux segments : les lois qui réglementent la surveillance faite par le gouvernement et les lois qui règlement la surveillance faite par le secteur privé. Force est de constater que la situation se complique encore plus, car les trois paliers de gouvernement (fédéral, provincial et territorial) peuvent adopter des lois pour régir la vie privée dans le secteur public et dans le secteur privé sur leur territoire.

Les mécanismes de collecte d'information utilisés par le gouvernement fédéral sont réglementés par la *Loi de 1982 sur la protection des renseignements personnels*. Cette *Loi* établit les règles que doivent suivre les organismes gouvernementaux pour la collecte, l'utilisation et la divulgation de renseignements personnels. Le commissaire à la protection de la vie privée, un agent indépendant du Parlement, supervise l'application de la *Loi* et est habilité à intenter des poursuites, à intervenir dans les procédures, à déposer des plaintes et à mener des enquêtes. Cependant, comme les pratiques relatives à l'information ont changé considérablement depuis 1982, la plupart des observateurs sont d'avis que la loi est dépassée et qu'elle devrait être réformée en profondeur pour que l'on puisse faire face aux problèmes relatifs à la vie privée qui ont été présentés dans cet ouvrage.

Par ailleurs, toutes les provinces ont adopté des lois pour réglementer le traitement des renseignements personnels par les organes publics provinciaux. Dans la plupart des provinces, ce sont les commissaires à l'information

et à la protection de la vie privée qui sont mandatés pour surperviser l'exécution de ces lois ainsi que des dispositions sur l'accès à l'information sur leur territoire respectif.

Les pratiques de collecte de l'information dans le secteur privé sont quant à elles sous réglementation fédérale, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), laquelle est entrée en vigueur en 2004. Cette *Loi* vise tous les organismes, y compris les entreprises étrangères qui recueillent, utilisent ou divulguent des renseignements personnels dans le cadre de leurs activités commerciales. Elle a été inspirée du *Code type sur la protection des renseignements personnels*[7] de l'Association canadienne de normalisation, lequel est assorti de dix principes relatifs à l'équité dans le traitement des renseignements personnels qui reflètent ceux d'autres lois et lignes directrices nationales et internationales.

En vertu de la *LPRPDE*, un organisme qui souhaite recueillir, utiliser ou divulguer les renseignements personnels d'une personne doit tout d'abord obtenir le consentement de ladite personne. De plus, lorsque les renseignements personnels sont de nature particulièrement délicate (dossier médical ou documents financiers), l'organisme doit obtenir un consentement explicite. Cependant, dans bon nombre de cas, on peut supposer que le consentement est implicite. Il s'agit donc de déterminer si, dans des circonstances similaires, une « personne raisonnable » s'attendrait à se faire demander si elle consent à la divulgation des renseignements.

Comme les dispositions reposant sur le consentement d'une « personne raisonnable » prévues dans la *LPRPDE* varient en fonction du contexte, les tribunaux doivent décider si le consentement peut être implicite dans chaque cas. À titre d'exemple, dans l'affaire *Englander* c. *Telus Communications Inc.* (2004 CAF 387, [2005] 2 RCF 572), un particulier a déposé une plainte au titre de la *LPRPDE* contre une compagnie nationale de téléphone[8]. L'appelant soutenait que l'entreprise avait omis d'indiquer qu'elle vend les renseignements sur les clients en format électronique à des entreprises externes de marketing. En pesant le droit à la vie privée du client et les besoins de l'entreprise, le tribunal a conclu que les nouveaux abonnés devaient être informés, avant que leur information ne soit rendue publique, qu'ils pouvaient choisir de ne pas faire publier leur numéro et ainsi empêcher que leur information soit vendue à des tiers. Autrement dit, les clients doivent adhérer explicitement à la collecte, l'utilisation et la divulgation de ce type de renseignements personnels.

Conformément à la *LPRPDE*, les entreprises doivent s'assurer que les renseignements personnels qu'elles recueillent sont « aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés ». De plus, l'information doit être stockée de façon sécurisée ; il faut notamment protéger les documents électroniques en les chiffrant et en conservant l'historique des accès. Enfin, les entreprises doivent donner, aux consommateurs qui en font la demande par écrit, l'accès à leur information personnelle conservée par l'entreprise pour que les erreurs dans cette information puissent être corrigées.

Bien que la *LPRPDE* soit une loi fédérale, elle s'applique également aux renseignements personnels amassés par les organismes sous réglementation provinciale, sauf si la province concernée a déjà adopté une loi « essentiellement similaire ». Le Québec, la Colombie-Britannique et l'Alberta ont promulgué de telles lois.

En somme, sauf quelques rares exceptions, tous les organismes au Canada sont assujettis à des dispositions législatives sur la protection des renseignements personnels. À quelques exceptions près, les données personnelles recueillies sur les citoyens canadiens sont encadrés par des principes d'équité élémentaire en matière de traitement de l'information. (Se reporter à l'Annexe 1 pour une analyse des principales lois sur la protection de la vie privée au Canada).

Ces lois sont-elles efficaces ? En toute honnêteté, elles ne le sont que « parfois ». Elles sont bourrées d'exemptions et de nuances qui sont difficiles à comprendre pour le citoyen moyen. Les commissariats à la protection de la vie privée sont en général en mal de ressources, ce qui les empêche de faire des efforts constants et proactifs d'éducation et d'exécution de la loi. De plus, pour la même raison, ils ne peuvent suivre le rythme rapide d'évolution de la technologie. Par ailleurs, le commissaire fédéral à la protection de la vie privée n'est pas habilité à obliger les organismes à se conformer à la loi. Or, même les commissaires provinciaux, qui sont investis de tels pouvoir, tendent à jouer principalement un rôle d'ombudsman ; ils reçoivent les plaintes des citoyens ordinaires, mènent des enquêtes en toute discrétion et confidentialité, et travaillent en coulisse avec les organismes publics et privés. Il n'est donc pas étonnant que le règlement des plaintes soit long.

Bon nombre de commissaires au Canada jouissent d'une très bonne réputation à l'étranger et dans l'opinion publique et ils font constamment la manchette des médias nationaux et locaux. En effet, certaines de leurs réussites ont eu un grand retentissement. En 2009, notamment, la commissaire fédérale à la protection de la vie privée, Jennifer Stoddart, s'est attaquée

à Facebook et l'a forcé à changer certaines de ses politiques[9]. En 2012, la commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique est parvenue à modifier le fonctionnement des caméras du système de reconnaissance automatique des plaques d'immatriculation dans la province[10]. Parfois, les commissaires à la protection de la vie privée joignent leurs efforts, comme ils l'ont fait pour contester le projet de loi sur l'accès légal présenté par le gouvernement (se reporter aux tendances 3 et 7). Ils commencent également à collaborer à des actions d'exécution de la loi sur la scène internationale[11].

Bien que les constestations judiciaires portent fruit, tous les observateurs seront probablement d'avis que les lois ne suffisent pas ou du moins que ces lois ne peuvent être efficaces que si elles sont appliquées dans une société qui affiche un respect fondamental de la vie privée. Les lois sur la protection de la vie privée exigent foncièrement que les organismes rendent des comptes quant aux données personnelles qu'ils traitent et que les citoyens se soucient de leur vie privée.

Par conséquent, un second facteur qui prend de l'importance est les mesures prises par les organismes eux-mêmes pour faire avancer le dossier de la vie privée. Il existe tout un éventail d'activités volontaires ou d'autoréglementation que les organismes peuvent entreprendre et qu'ils ont déjà entreprises. Dans le secteur privé, on affirme maintenant couramment que la protection de la vie privée est une bonne pratique d'affaires. Le raisonnement des entreprises est en quelque sorte le suivant : les entreprises ont besoin que les consommateurs aient confiance en elles. Une gestion adéquate des renseignements personnels est donc essentielle pour obtenir et conserver cette confiance. Par conséquent, en indiquant sur son site Web « la protection de votre vie privée est importante pour nous », l'entreprise qui possède le site prend cet engagement pour que les clients voient qu'elle est digne de confiance. Certaines entreprises apposent même le sceau « Good Housekeeping Seal of Approval » sur leur site Web. Cependant, les organismes qui font cette promesse quant à la protection des renseignements personnels doivent être en mesure de la tenir.

Aujourd'hui, une importante communauté de professionnels dans le domaine de la protection de la vie privée a été mise en place pour aider les organismes à se conformer aux diverses lois sur la protection de la vie privée et à améliorer leur réputation en matière de protection des renseignements personnels. D'ailleurs, la section canadienne de l'International Association of Privacy Professionals (IAPP) se compose de consultants, de vérificateurs,

d'avocats, d'agents spécialisés dans la conformité à l'étranger et de technologues ; tous ces acteurs ont un intérêt professionnel dans le dossier et ils créent et échangent des pratiques exemplaires de gestion adéquate de la protection de la vie privée et d'évaluation des risques[12].

Bien entendu, la protection de la vie privée n'est importante que dans certains contextes et dans certains cas. Et souvent, elle se heurte à des conflits titanesques avec divers impératifs organisationnels et technologiques qui favorisent la surveillance. Reste que le fait de ne pas tenir compte de la protection de la vie privée peut nuire aux intérêts commerciaux. Les violations massives des données ne font rien pour aider les entreprises à maintenir leur réputation ou le cours des actions, pas plus qu'une décision défavorable ou une sanction d'un organe de réglementation. Il existe donc de réels motifs qui poussent les entreprises à prendre la protection de la vie privée au sérieux.

Cependant, les motivations sont en quelque sorte différentes dans le secteur public. Les organismes gouvernementaux tiennent particulièrement à éviter la mauvaise publicité associée aux violations de données et mettent donc tout en œuvre pour éviter ces infractions. D'ailleurs, nombre d'organismes fédéraux et provinciaux doivent produire une évaluation des facteurs relatifs à la vie privée et essaient ainsi de s'assurer que la vie privée est protégée lorsqu'une nouvelle politique est mise en œuvre. Ces évaluations sont censées donner aux organismes un cadre uniforme pour l'évaluation de l'incidence sur le droit et les facteurs liés à la vie privée des politiques et des procédures ministérielles. La plupart du temps, ces évaluations prennent la forme de listes de vérification typiques qui servent à rendre légitimes les nouveaux programmes plutôt qu'à les soumettre à un examen approfondi et rigoureux.

Une autre façon de protéger la vie privée consisterait à l'incorporer aux systèmes de collecte et d'utilisation de l'information. Avec tous les exemples cités dans cet ouvrage, vous croirez peut-être que la technologie est à la base du problème, en particulier la technologie qui est hors de contrôle et qui évolue à son propre rythme en laissant derrière l'analyse sociale et les recours juridiques. Il s'agit en effet d'un important chapitre de l'histoire. Par contre, il est possible de modeler la technologie afin qu'elle protège la vie privée ou qu'elle lui porte atteinte.

Le concept de la « protection intégrée de la vie privée » (PIP) est maintenant admis généralement au sein de toute la communauté des professionnels du domaine de la vie privée. La commissaire à l'information et à la protection

de la vie privée de l'Ontario, Ann Cavoukian, a défendu énergiquement l'idée. La protection intégrée de la vie privée repose sur sept principes :

(1) prendre des mesures proactives plutôt que réactives
(2) s'assurer que la protection de la vie privée est la position de départ
(3) intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
(4) assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
(5) assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
(6) assurer la visibilité et la transparence
(7) respecter les utilisateurs[13].

La PIP avait comme point de départ le constat que bon nombre d'organismes n'ont pas réellement *besoin* de données personnelles identifiables pour s'acquitter de leurs fonctions de base. En d'autres termes, il est possible de conjuguer sécurité *et* protection de la vie privée dans une conception adéquate et proactive. Un bon exemple est un système de vidéosurveillance qui chiffrerait par défaut les images et en autoriserait le déchiffrement seulement si un crime est commis et que la police a obtenu un mandat. Ce genre de système peut coûter cher et sa mise au point se concilie mal avec le réflexe naturel des organismes de recueillir le plus d'information possible. Néanmoins, de nombreux faits concourent à indiquer que la technologie peut être conçue pour assurer la protection plutôt que pour porter atteinte à la vie privée et que la vie privée peut faire partie des paramètres par défaut. La technologie peut donc faire partie de la solution.

De nos jours, des technologies d'amélioration de la confidentialité (TAC) sont maintenant offertes gratuitement aux simples citoyens. Certaines sont assez élémentaires, ne requièrent pas d'habiletés techniques et peuvent être utilisées sans hésiter ; la plupart d'entre nous n'aiment pas que les passants épient par les fenêtres de notre maison, nous fermons alors les rideaux. Les rideaux ont maintenant un équivalent pour nous protéger des regards indiscrets dans le monde virtuel : les programmes de cryptage des courriels et les services de courriels anonymes ; les fonctions de navigation privée dans la plupart des fureteurs qui empêchent les fichiers de témoins d'être enregistrés ; les filtres antipourriel ; et les systèmes Do Not Track qui empêchent les annonceurs externes de suivre nos habitudes de navigation. De nos jours, il

n’est pas nécessaire d’être un spécialiste de la technologie pour utiliser ces programmes. Au fil des ans, ils se sont répandus et sont devenus très conviviaux. (Se reporter à l’Annexe 3 pour une liste des outils en ligne les plus couramment utilisés pour protéger la vie privée.)

Ces exemples montrent que les citoyens peuvent prendre eux-mêmes des mesures pour protéger leur vie personnelle et pour obliger les organismes à rendre des comptes. Les organismes gouvernementaux et les entreprises nous demandent souvent de fournir des données personnelles excessives ou non pertinentes, alors que les lois canadiennes sur la protection de la vie privée stipulent que l’information recueillie doit être appropriée ou proportionnelle aux besoins organisationnels. Le simple fait de demander à un organisme pourquoi il a besoin de vos renseignements personnels peut être un moyen efficace pour sensibiliser l’organisme et ses employés. En 2012, un locataire potentiel s’est notamment plaint lorsque le propriétaire de l’immeuble lui a demandé son numéro d’assurance sociale sur le formulaire de demande de location en Alberta. La commissaire à l’information et à la protection des renseignements personnels de l’Alberta a interdit cette pratique en faisant valoir que le numéro d’assurance sociale n’était d’aucune utilité pour déterminer si le candidat constitue un locataire approprié[14].

De la même façon, dans le secteur privé, les Canadiens peuvent décider d’acheter des biens et de retenir les services uniquement d’entreprises qui respectent leurs droits et intérêts en matière de vie privée. Si un consommateur estime qu’une entreprise a violé ses droits protégés par la loi, il peut signaler cette présumée violation au commissaire à la vie privée provincial ou fédéral qui a compétence. Ce consommateur peut aussi tout bonnement cesser de faire affaire avec l’entreprise.

Certaines recherches montrent que les particuliers tentent souvent de résister à la surveillance. Le sociologue Gary Marx s’est d’ailleurs penché sur les nombreux moyens ingénieux qu’ont trouvés les particuliers pour éviter ou contrecarrer les initiatives de surveillance : ils brouillent leur identité, déforment leurs données, refusent de se conformer, etc[15]. Certains défenseurs de la vie privée plus radicaux ont poussé cette résistance un peu plus loin. Les gens ordinaires commencent notamment à observer les personnes et les organismes qui les surveillent et à étayer leurs actions. Prenons l’exemple d’une personne qui utiliserait son téléphone intelligent pour filmer un policier qui emploierait des méthodes abusives. Un autre exemple serait la cartographie des caméras de surveillance dans une ville et la publication de cette carte.

Au-delà de la résistance individuelle, il est possible de mener une action collective par l'intermédiaire d'organisations de la société civile[16]. Les organisations de défense de la vie privée ont adopté plusieurs stratégies différentes : elles utilisent les médias en ligne et hors-ligne pour dénoncer les problèmes et soulever les enjeux ; elles déposent des plaintes auprès des commissaires à la vie privée ; elles participent à d'importants projets de recherche ; elles font la promotion des initiatives d'éducation ; et elles soumettent des demandes d'accès à l'information. Bien qu'elles disposent de maigres ressources, elles peuvent informer, gêner, éduquer et utiliser leur influence lorsque les mesures de surveillance deviennent excessives. La campagne « Arrêtez l'espionnage en ligne », qui a été menée contre le projet de loi sur l'accès légal présenté par le gouvernement et qui a été citée dans les troisième, septième et neuvième tendances en est un exemple. Le succès remporté par ces initiatives met en évidence le rôle important que peut jouer l'éducation du public dans la promotion de meilleures politiques de protection de la vie privée.

Nos enfants doivent également être sensibilisés à l'importance de la vie privée. L'organisme non gouvernemental canadien, MediaSmarts, conçoit et offre des outils éducatifs primés sur la protection de la vie privée à l'intention des jeunes Canadiens depuis 1996. MediaSmarts collabore avec les écoles et les bibliothèques de partout au pays en vue d'enseigner aux jeunes comment évaluer avec un œil critique l'incidence de la surveillance dans leur école, au centre commercial et sur les médias sociaux. L'organisme aide également les jeunes à comprendre l'importance de la protection de la vie privée dans la citoyenneté démocratique. Nous pouvons être fiers de ce fleuron canadien puisque des organismes de littératie numérique en Europe et aux États-Unis ont pris exemple sur celui-ci.

N'oublions pas que certaines formes de surveillance sont tout simplement stupides, intéressées ou inutiles, des cibles parfaites pour le sarcasme et la satire. L'humour joue et jouera toujours un rôle important et crucial pour dénoncer les bizarreries de notre culture de surveillance. D'ailleurs, en 2003 et 2006, l'organisme non gouvernemental, Privacy International, a remis le « Stupid Security Award » aux cas les plus flagrants de mesures de sécurité absurdes[17]. Il est facile de se moquer de ces exemples, car ils sont bien visibles.

Cependant, la surveillance est devenue anodine, intégrée et de moins en moins visible, même si elle devient de plus en plus banale. La surveillance est généralement une technique pour exercer un pouvoir et un contrôle social qui repose sur la grande visibilité de la personne observée et sur l'invisibilité relative de la personne qui observe. Elle est également conçue pour

accroître l'influence de l'observateur sur la personne ou le groupe observé. Peu importe si l'application d'un tel pouvoir est légitime ou inoffensive, elle vient inévitablement bousculer les normes démocratiques libérales qui reposent sur l'autonomie citoyenne.

La manière conventionnelle de s'attaquer à de telles tensions est par l'ouverture, le débat public et la supervision. L'absence de ce type de mesures de réglementation ouvre la porte aux abus et à la corruption ; les observateurs qui sont privilégiés exploitent de façon inappropriée les personnes qui ont moins d'influence et, par conséquent, ont encore plus de raison de vouloir cacher leurs activités. Ce phénomène entraîne un risque particulier lorsque la surveillance est intégrée aux objets et aux immeubles de la vie de tous les jours ; de telles pratiques sont rarement visibles de l'extérieur et sont généralement combinées à des activités plus légitimes desquelles elles dépendent. L'ouverture et la transparence sont donc indispensables pour que les responsables de la surveillance soient tenus de rendre des comptes de façon objective.

Nous avons décrit une vaste gamme d'approches et d'outils : lois, autoréglementation, technologies d'amélioration de la confidentialité, sensibilisation des consommateurs, résistance individuelle et activisme collectif. Chacune de ces stratégies peut être efficace selon le contexte. Elles sont toutes nécessaires, mais, prises isolément, aucune ne peut suffire. Alors, tous ces moyens d'action pourraient-ils être combinés en une stratégie politique ? La politique de la vie privée ou de « l'antisurveillance » existe-t-elle[18] ? Il ne fait aucun doute que les Canadiens se soucient de la protection de leur vie privée et que les politiciens qui seraient portés à l'oublier pourraient déclencher un déluge de critiques. Comme nous en avons fait état à la Tendance 7, c'est exactement ce qui s'est produit lorsque le gouvernement fédéral a tenté d'adopter le projet de loi C-30 sur la surveillance en ligne.

Les Canadiens du XXIe siècle ont tous expérimenté la surveillance de masse. Leur vie est maintenant transparente pour bon nombre d'organismes. Ce phénomène change le cours des choses puisque non seulement il compromet notre vie privée, mais il pourrait également limiter nos possibilités et nos ambitions. La surveillance nous accapare tous profondément ; elle ne se limite plus qu'aux « suspects » ou aux personnes qui auraient « quelque chose à cacher ». L'exemple de la petite Farah présenté dans la première tendance nous prouve que dans la vie de tous les jours, avec la famille et avec les amis, la surveillance s'est transformée en une réalité persistante, pour le meilleur et pour le pire. Le privé est politique.

L'enjeu politique entourant les données personnelles consiste principalement à garantir la transparence des processus de surveillance. Cette démarche touche tous les niveaux et une vaste série d'acteurs. Bien entendu, nous devrions nous-mêmes être plus conscients de la surveillance à laquelle nous sommes assujettis, que nous traitions des données ou que nous divulguions notre information personnelle. Or, il serait tout à fait inadéquat, voire risible, de demander aux Canadiens ordinaires de tenter de découvrir comment ils sont surveillés et de prendre les mesures qui s'imposent dans le contexte actuel. Il incombe plutôt aux responsables de la surveillance d'assumer leurs responsabilités à l'égard des personnes dont les données sont traitées et de rendre leurs pratiques transparentes pour ceux qui sont touchés. Ceux qui manipulent et reconfigurent nos données personnelles, que ce soit pour générer des profits ou pour maintenir l'ordre, devraient également nous rendre des comptes. Voilà ce qu'exigent les lois canadiennes. Or, en pratique, les lois sont plus laxistes et renferment trop de failles.

Cet ouvrage tire la sonnette d'alarme. Nous devons être vigilants par rapport aux tendances décrites ici, nous devons prendre conscience de notre complicité dans ces tendances et nous devons être prêts à parler au nom de ceux qui subissent les effets négatifs de la surveillance contemporaine. Bien qu'il soit évident que la surveillance nous touche tous, elle porte davantage préjudice à certains groupes et à certaines personnes. Les grands organismes qui traitent des données personnelles doivent donc être tenus responsables de leurs activités. En somme, aucune de ces tendances n'est inévitable. Le phénomène de la surveillance est réversible. La vie privée n'a pas été anéantie.

Notes

1 Voir Polly Sprenger, « Sun on Privacy: 'Get Over It' », *Wired,* 26 janvier 1999, http://www.wired.com/politics/law/news/1999/01/17538.

2 Beverley McLachlin et coll., *R.* c. *Tessling*, Jugements de la Cour suprême, Cour suprême du Canada, 2004 (paragraphe 21), http://scc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/fr/item/2183/index.do.

3 Ibid., paragraphe 25.

4 Ibid., paragraphe 23 (citation de Alan F. Westin, *Privacy and Freedom* [New York, Atheneum, 1967], p. 7).

5 *R. c. A.M.,* [2008] 1 RCS 569, 2008 CSC 19.

6 Voir, par exemple, Albert Kramberger, « Hydro's New Smart Meters Sparks Opposition in West Island », *Gazette*, Montréal, 15 avril 2013, http://westislandgazette.com/news/story/2013/04/15/

hydros-new-smart-meters-sparks-opposition-in-west-island/ ; et site Web de la Coalition to Stop Smart Meters de la Colombie-Britannique, http://www.stopsmartmetersbc.ca/html/.

7 Les principes du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation s'inspirent en retour de documents produits antérieurement par l'Organisation de coopération et de développement économiques (OCDE). Se reporter aux *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de la Direction de la science, de la technologie et de l'industrie de l'OCDE (Paris, OECD, 1980).

8 *Englander* c. *Telus Communications Inc.,* [2005] 2 RCF 572, 2004 CAF 387.

9 Canada, Commissariat de la protection de la vie privée, « Document d'information » ; *Conclusions détaillées des enquêtes sur Facebook*, 4 avril 2012, http://www.priv.gc.ca/media/nr-c/2012/bg_120404_f.asp.

10 Elizabeth Denham, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, « Use of Automated License Plate Recognition Technology by the Victoria Police Department », *Rapport d'enquête F12-04*, 15 novembre 2012, http://www.oipc.bc.ca/report/investigation-reports.aspx. Voir aussi Rob Shaw, « Privacy Commissioner Orders Victoria Police to Change Automated Licence Plate Recognition », *Times Colonist,* Victoria, 15 novembre 2012, http://www.timescolonist.com/news/privacy-commissioner-orders-victoria-police-to-change-automated-licence-plate-recognition-1.24535.

11 Sur les initiatives du Global Privacy Enforcement Network, se reporter au site Web de l'organisme, https://www.privacyenforcement.net/.

12 Sur les travaux de l'International Association of Privacy Professionals du Canada, se reporter au site Web de l'organisme, https://www.privacyassociation.org/community/iapp_canada.

13 Voir Ontario, Commissaire à l'information et à la protection de la vie privée, *Sept principes fondamentaux*, Protection intégrée de la vie privée, Toronto, 2013, http://www.viepriveeintegree.ca/index.php/a-propos-de-la-pivp/sept-principes-fondamentaux/.

14 Alberta, Commissaire à l'information et à la protection de la vie privée, ordonnance P2012-11, 15 novembre 2012, « G.M.A. Properties Inc. / Alliance Realty Inc. », http://www.oipc.ab.ca/downloads/documentloader.ashx?id=3125.

15 Gary T. Marx, « A Tack in the Shoe: Resisting and Neutralizing the New Surveillance », *Journal of Social Issues* 59, nº 2, 2003, p. 369-390.

16 Parmi ces organismes, citons la BC Civil Liberties Association, la BC Freedom of Information and Privacy Association, l'Association canadienne des libertés civiles, la Clinique d'intérêt public et de politique d'Internet du Canada, la Coalition pour la surveillance internationale des libertés civiles, la Ligue des droits et libertés, OpenMedia.ca, et le Centre pour la défense de l'intérêt public. Se reporter à l'annexe 4 pour une liste complète.

17 Voir, par exemple, John Leyden, « Gongs on Offer for Stupid Security Measures », *The Register,* 22 août 2006, http://www.theregister.co.uk/2006/08/22/stupid_security_awards/ ; « Stupid Security Awards 2006 », *DaniWeb,* http://www.daniweb.com/hardware-and-software/networking/news/218098/stupid-security-awards-2006.

18 Voir Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA, MIT Press, 2008).

ANNEXES

Foire aux questions sur la surveillance et les lois sur la protection de la vie privée

Dans cette annexe, nous répondrons aux questions les plus courantes au sujet de la surveillance effectuée par les gouvernements, les entreprises et les particuliers, à la lumière de certaines des lois qui protègent le droit à la vie privée. Les lois peuvent se révéler très complexes, peuvent varier selon la province ou le territoire et peuvent changer au fil du temps. Par conséquent, les réponses suivantes ne sont que des renseignements généraux et préliminaires.

Comment l'information personnelle que je fournis aux entreprises est-elle protégée ?

Lorsqu'une entreprise recueille et utilise vos renseignements personnels, la loi vous autorise à demander pourquoi elle en a besoin : une société peut amasser uniquement l'information qui est essentielle à l'exercice de ses fonctions de base. Vous avez le droit de voir les renseignements qu'une entreprise détient sur vous pour en vérifier l'exactitude et de retirer votre consentement. En règle générale, une entreprise qui souhaite recueillir de l'information personnelle de nature délicate (dossiers médical ou financier) doit tout d'abord obtenir votre consentement explicite. Par ailleurs, les entreprises doivent protéger ces renseignements. Enfin, elles doivent désigner une personne qui sera responsable des pratiques organisationnelles de collecte

de l'information et fournir ses coordonnées. Pour plus d'information sur vos droits au titre de la principale loi fédérale qui conditionne les pratiques organisationnelles de collecte de l'information, la *Loi sur la protection des renseignements personnels et les documents électroniques*, se reporter au guide à l'adresse suivante : http://www.priv.gc.ca/information/02_05_d_08_f.asp.

Si vous estimez que vos renseignements personnels ont été mal protégés par une entreprise, vous pouvez déposer une plainte auprès du Commissaire à la vie privée du Canada : http://www.priv.gc.ca/complaint-plainte/pipeda_f.asp.

En Colombie-Britannique, en Alberta et au Québec, les commissaires à la vie privée provinciaux sont également habilités à mener des enquêtes sur les plaintes visant des entreprises au titre des lois provinciales applicables :

- Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique
  http://www.oipc.bc.ca/
- Bureau du commissaire à l'information et à la protection de la vie privée de l'Alberta
  http://www.oipc.ab.ca/pages/home/default.aspx
- Commission d'accès à l'information du Québec
  http://www.cai.gouv.qc.ca/

Dans les autres provinces, la *Loi sur la protection des renseignements personnels et les documents électroniques* s'applique ; vous devrez donc déposer votre plainte au Commissariat de la protection de la vie privée du Canada.

Comment les renseignements personnels que je fournis au gouvernement sont-ils protégés ?

Le gouvernement fédéral ainsi que celui des provinces et des territoires imposent des restrictions quant à la collecte et à l'échange de renseignements personnels par tous les paliers de gouvernement. De plus, certaines provinces, comme l'Ontario, ont adopté des mesures extraordinaires de protection pour l'information sur la santé (se reporter au site Web de la Commissaire à l'information et à la protection de la vie privée de l'Ontario, à http://www.ipc.on.ca/french/home-page/default.aspx).

En règle générale, ces lois exigent que les organismes gouvernementaux se dotent de politiques pour la collecte et l'utilisation des renseignements personnels, qu'ils les rendent accessibles au public et qu'ils fassent en sorte que ces politiques soient compréhensibles. Conformément à ces lois, les organismes gouvernementaux sont également tenus de ne recueillir que l'information nécessaire à la prestation de leurs services, tel qu'autorisé par la loi. Les dispositions législatives sur la protection de la vie privée restreignent la mesure dans laquelle ces organismes peuvent partager cette information. Habituellement, ces mêmes dispositions autorisent une personne à demander aux organismes gouvernementaux quels renseignements ils ont recueillis et conservés à son sujet, à les examiner et à faire modifier les renseignements qui ne sont pas exacts.

Si vous estimez que vos renseignements personnels ont été glanés, stockés ou communiqués de façon inappropriée par un organisme gouvernemental provincial, vous pouvez déposer une plainte auprès du commissaire à la protection de la vie privée ou à l'ombudsman de votre province ; celui-ci est habilité à recevoir les plaintes et à les régler. Pour une liste des entités gouvernementales des provinces responsables de la protection de la vie privée, se reporter à : http://www.priv.gc.ca/resource/prov/index_f.asp.

Par ailleurs, si vous estimez qu'un organisme fédéral a traité de façon inadéquate vos renseignements personnels, vous pouvez déposer une plainte auprès du Commissariat à la protection de la vie privée du Canada. Pour les directives à suivre et les formulaires à remplir, se reporter à :
http://www.priv.gc.ca/complaint-plainte/pa_f.asp

Puis-je poursuivre en justice un particulier qui porte atteinte à ma vie privée ?

Au Canada, quatre provinces (Colombie-Britannique, Saskatchewan, Manitoba, et Terre-Neuve-et-Labrador) ont adopté des lois qui font de l'atteinte à la vie privée un délit civil (on entend par délit civil un acte fautif qui peut engendrer une poursuite civile)*. Un délit civil fait généralement l'objet d'une poursuite entreprise par la personne qui a été visée par la sur-

* En Colombie-Britannique, la loi est le *Privacy Act*, RSBC 1996, c. 373 ; en Saskatchewan, il s'agit du *Privacy Act*, RSS 1978, c. P-24 ; au Manitoba, il s'agit de la *Loi sur la protection de la vie privée*, CCSM c. P125 ; et à Terre-Neuve-et-Labrador, il s'agit du *Privacy Act*, RSNL 1990, c. P-22.

veillance audio ou vidéo, d'usurpation d'identité, ou dont les documents ont été consultés ou utilisés.

Dans l'affaire *Jones* c. *Tsige*, 2012 ONCA 32, la Cour d'appel de l'Ontario a confirmé l'existence d'un délit civil d'atteinte à la vie privée (on parle alors de droit jurisprudentiel). Les Ontariens peuvent donc intenter une poursuite, s'ils estiment qu'une atteinte illégale a été portée à leur vie privée. L'action contre l'intrusion dans l'intimité doit présenter trois éléments :

- une conduite intentionnelle de la part du défendeur (y compris un comportement inconsidéré) ;
- une ingérence, sans justification légitime, dans les affaires privées ;
- une personne raisonnable considérerait l'invasion comme étant très choquante et causant de la détresse, de l'humiliation ou de l'angoisse.

Suis-je obligé de m'identifier aux policiers ?

En général, bien qu'il soit tout à fait acceptable pour les policiers d'engager la conversation avec vous et de vous poser des questions, vous n'êtes pas tenu de leur fournir l'information. Dans certains cas, toutefois, vous êtes tenu de vous identifier aux policiers. Dans l'affaire *Moore* c. *La Reine [1979] 1 R.C.S. 195*, la Cour suprême a confirmé les accusations en soutenant que le refus de s'identifier à un policier qui veut donner une contravention pour une infraction à la circulation constitue une entrave au travail du policier. Si un policier soupçonne une infraction précise, vous avez vraisemblablement l'obligation de fournir votre nom et vos coordonnées.

Quelle information suis-je tenu de fournir aux policiers ?

Si vous êtes suspect, détenu pour un interrogatoire ou arrêté, vous jouissez de plusieurs protections au titre de la common law (le droit jurisprudentiel) et des lois constitutionnelles (la *Charte des droits et libertés*). Vous n'êtes pas tenu de répondre aux questions et, dès votre arrestation, vous devez être informé de votre droit de consulter un avocat. Vous avez le droit de garder le silence et les policiers ne peuvent vous forcer à répondre lors

d'une enquête. Cependant, un policier a le droit d'interroger une personne après qu'elle a consulté un avocat, et ce, même si la personne revendique son droit de garder le silence. Enfin, un policier peut observer une personne arrêtée ou détenue et utiliser les conversations qu'elle a eues avec d'autres détenus.

Quand les policiers peuvent-ils faire une fouille ?

En vertu de l'article 8 de la *Charte canadienne des droits et libertés*, « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». En règle générale, on part du principe que les policiers doivent obtenir un mandat pour faire une fouille ou une perquisition. Chaque fois que vous avez le *droit de vous attendre raisonnablement à ce que votre vie privée soit protégée*, les policiers doivent obtenir une autorisation judiciaire d'un juge indépendant ou d'un juge de la paix pour être autorisés à transgresser votre vie privée. Les policiers doivent donc présenter des motifs raisonnables et probables à un décideur impartial pour avoir l'autorisation de procéder à une fouille de vos effets personnels ou de votre maison. On entend par motifs raisonnables et probables, les cas où il est raisonnable de croire qu'une infraction a été commise et que des preuves pertinentes seront obtenues au moyen de la preuve ; de simples soupçons ne suffisent pas, comme on l'a établi dans l'affaire *Hunter et autres* c. *Southam Inc. [1984] 2 R.C.S. 145*.

Peut-on me fouiller si je suis arrêté ou détenu ?

Les policiers sont autorisés à fouiller une personne immédiatement après son arrestation. Ils le font pour s'assurer que la personne arrêtée n'est pas en possession d'une arme ou d'une autre matière dangereuse. De plus, les policiers ont aussi la chance de recueillir des preuves qui auraient pu être détruites s'ils avaient dû obtenir un mandat.

Dans l'affaire *R.* c. *Caslake [1998] 1 R.C.S. 51*, le droit de faire une fouille après l'arrestation a été limité aux fouilles qui étaient réellement accessoires à l'arrestation. Les juges ont statué que les fouilles qui ne sont qu'une formalité administrative et qui n'ont aucun lien avec les circonstances véritables de l'arrestation enfreignent l'article 8. Dans l'affaire *R.* c. *Stillman [1997] 1 R.C.S.*

607, la Cour suprême a jugé que le droit de procéder à une fouille accessoire à l'arrestation n'incluait pas le prélèvement d'échantillons de substances corporelles sur la personne arrêtée.

Si une personne est détenue, plutôt qu'arrêtée, les policiers ont beaucoup moins de pouvoirs pour la fouille. Dans l'affaire *R.* c. *Mann [2004] 3 R.C.S. 59, 2004 CSC 52*, la Cour suprême a décidé que, lorsque les policiers ont des motifs raisonnables d'établir un lien entre une personne et un crime donné, ils peuvent procéder à la détention de cette personne et, dans le cadre de cette détention, ils peuvent soumettre cette personne à une simple fouille par palpation, pour assurer la sécurité des policiers ; ils ne peuvent le faire que pour cette raison.

Puis-je être soumis à une fouille à nu ?

Les policiers sont autorisés à procéder à des fouilles à nu. Dans l'affaire *R.* c. *Golden [2001] 3 R.C.S. 679, 2001 CSC 83*, la Cour suprême a statué que, outre le fait que l'arrestation doit se faire sur la base de motifs raisonnables et probables, les policiers doivent avoir des motifs raisonnables et probables de croire que dans le cadre de la fouille accessoire à l'arrestation une fouille à nu est nécessaire.

Les fouilles à nu sont considérées comme le type de fouille portant le plus atteinte à la vie privée. Par conséquent, elles doivent toujours être faites dans un endroit privé, comme un poste de police. Une fouille à nu est permise sur les lieux de l'arrestation en cas d'urgence uniquement.

Quand une perquisition peut-elle être faite dans ma maison ?

Votre maison est censée être l'endroit où vous jouissez du plus haut niveau de vie privée. Normalement, les policiers ne peuvent ni y entrer, ni y faire une perquisition sans avoir de mandat. Toutefois, les policiers sont autorisés à pénétrer dans une maison sans mandat dans certaines circonstances précises. En cas d'urgence, les policiers peuvent entrer dans une maison pour arrêter un suspect, si pendant qu'ils attendent le mandat, des preuves risquent d'être détruites ou si la sécurité d'autres personnes est en jeu. Pour les appels au 911, les policiers sont autorisés à fouiller l'endroit d'où l'appel a été fait seulement et peuvent entrer sans avoir de mandat.

Quand les policiers peuvent-ils fouiller ma voiture ?

Dans l'affaire *R.* c. *Caslake [1998] 1 R.C.S. 51*, les policiers ont décidé que les personnes se trouvant dans une voiture devaient s'attendre à ce que leur vie privée soit inférieure à celle qu'elles auraient dans leur maison. Par conséquent, la fouille d'une voiture peut être accessoire à l'arrestation d'une personne (on suppose dans ce cas-ci que la personne se trouvait à l'intérieur ou près de la voiture au moment de l'arrestation). Si un policier arrête une personne pour un motif relatif à la conduite du véhicule, la fouille du véhicule doit se limiter aux objectifs du contrôle routier seulement comme on l'a établi dans l'affaire *R.* c. *Mellenthin [1992] 3 R.C.S. 615*.

Dans l'affaire *Dedman* c. *La Reine [1985] 2 R.C.S. 2*, la Cour suprême a statué que les policiers ont l'obligation d'assurer la sécurité des personnes qui utilisent les voies publiques et que, par conséquent, ils avaient le pouvoir d'arrêter au hasard des véhicules pour vérifier si un conducteur a bu ou s'il a commis une infraction. Les policiers n'ont donc besoin que de très peu de motifs pour arrêter une voiture et procéder à une fouille en vue de repérer une infraction de la circulation.

Mon téléphone ou mon ordinateur peuvent-ils être fouillés ?

Dans l'affaire *R.* c. *Fearon,* 2013 ONCA 106, la Cour d'appel de l'Ontario a décidé qu'il est acceptable que les policiers fassent une fouille superficielle d'un téléphone cellulaire accessoirement à une arrestation, si ce téléphone n'est pas verrouillé ou protégé par mot de passe. Pour aller au-delà d'une fouille superficielle ou pour fouiller un téléphone verrouillé, les policiers doivent obtenir un mandat.

Pour les mandats de perquisition, un ordinateur portable ou un téléphone intelligent est considéré comme un endroit distinct de l'emplacement où il se trouve. Par conséquent, si un mandat est lancé pour une maison ou une voiture et que les policiers y trouvent un ordinateur ou un téléphone intelligent, ils ne peuvent y faire de fouille avant qu'un autre mandat ne soit obtenu.

Les policiers peuvent-ils fouiller mes poubelles ?

Dans l'affaire *R.* c. *Patrick*, 2009 CSC 17, la Cour suprême a accepté que les policiers utilisent des preuves obtenues dans des sacs d'ordures que l'accusé avait placés aux limites de son terrain pour le ramassage par la municipalité. Le juge a conclu que l'accusé n'avait pas une attente raisonnable au respect de sa vie privée à l'égard des objets pris dans les ordures qu'il avait placées en vue du ramassage.

Les policiers sont-ils autorisés à utiliser des chiens renifleurs ?

Dans l'affaire *R.* c. *Kang-Brown, 2008 CSC 18,* la Cour suprême a permis l'utilisation de chien renifleur dans une gare d'autobus pour faire des fouilles au hasard, s'il y a des motifs raisonnables de croire que des activités illicites s'y produisent. Des critères inférieurs à ceux normalement appliqués pour l'obtention d'un mandat d'un juge ont été appliqués. Il faut toutefois mentionner que les enfants peuvent plus s'attendre à ce que leur vie privée soit protégée à l'école ; c'est pourquoi les fouilles au hasard ne sont pas permises dans cette situation comme on l'a établi dans l'affaire *R. c. A.M., 2008 CSC 19*.

Les policiers peuvent-ils prélever des échantillons d'ADN et combien de temps peuvent-ils les conserver ?

Des éléments de preuve provenant de l'analyse de l'ADN peuvent être recueillis et utilisés par les policiers au cours d'une enquête, mais les policiers doivent obtenir préalablement un mandat*. De plus, la liste déjà longue des infractions pour lesquelles des éléments de preuve provenant de l'analyse de l'ADN peuvent être recueillis ou peuvent être recueillis après les accusations selon la décision d'un juge continue de s'allonger.

Dans certains cas, les éléments de preuve provenant de l'analyse de l'ADN conservés doivent être détruits ou pourraient être détruits si le commissaire de la GRC le juge utile. Les éléments de preuve provenant de

* *Code criminel*, LRC 1985, c C-46, art. 487.05, http://canlii.ca/fr/ca/legis/lois/lrc-1985-c-c-46/104133/lrc-1985-c-c-46.html#art487.05.

l’analyse de l’ADN doivent être détruits immédiatement si l’ordonnance qui autorisait leur prélèvement est déclarée nulle ou si la personne concernée est acquittée des accusations pour lesquelles le prélèvement des preuves avait été ordonné. Les éléments de preuve provenant de l’analyse de l’ADN doivent être détruits en cas d’absolution inconditionnelle ou trois ans après l’absolution sous conditions, sauf si une autre ordonnance autorise le prélèvement et la conservation des éléments de preuve provenant de l’analyse de l’ADN de cette personne*. Un refus de détruire les éléments de preuve provenant de l’analyse de l’ADN peut faire l’objet d’un contrôle judiciaire.

* *Loi sur l’identification par les empreintes génétiques*, L.C. 1998, ch. 37, par. 9(2), http://canlii.ca/fr/ca/legis/lois/lc-1998-c-37/102285/lc-1998-c-37.html#art9.

Films sur la surveillance

Beaucoup de films populaires ont traité de la surveillance. Les films figurant dans cette annexe conviennent à un public adolescent et constituent une bonne façon de sensibiliser les jeunes des écoles secondaires ou des universités à ce phénomène.

Bienvenue à Gattaca (1997) – Ce film présente une vision dystopique d'un avenir génétiquement construit, dans lequel les citoyens sont classés et suivis en fonction de leur code génétique. Le personnage principal, qui dès sa naissance a été relégué à une sous-classe en raison de son code génétique, change de place avec un homme génétiquement amélioré pour prendre part à une mission dans l'espace.

Brazil (1985) – Ce film raconte l'histoire d'un homme vivant dans un monde rétrofuturiste qui est accusé de terrorisme par suite d'une erreur technique dans le système de surveillance de l'État. Un bureaucrate tentera de corriger l'erreur et deviendra lui-même un ennemi de l'État.

Conversation secrète (1974) – Ce classique réalisé par Francis Ford Coppola raconte l'histoire d'un expert de la surveillance qui est obsédé par sa propre vie privée alors qu'il s'efforce d'un protéger un couple qu'il a placé sous surveillance.

Fenêtre sur cour (1954) – Ce classique d'Hitchcock porte sur les liens entre la surveillance, le voyeurisme et la vie privée en racontant l'histoire d'un reporter qui est contraint de rester chez lui pendant qu'il se rétablit d'une blessure.

Das Leben der Anderen (***La vie des autres,*** 2006) – L'histoire se déroule en 1984 à Berlin-Est et raconte la vie d'un écrivain, de son amie de cœur et d'un agent de la police secrète qui cache des micros dans l'appartement du premier. Ce film nous donne un excellent aperçu de la mécanique de la surveillance exercée par le bloc communiste ; il nous aide à prendre conscience de l'exercice du pouvoir et fait une lecture empathique des partisans de la vision orwélienne selon laquelle on peut exercer un contrôle en sachant tout.

L'œil du mal (2008) – Deux inconnus sont réunis lorsque les technologies qu'ils emploient au quotidien sont utilisées pour les suivre et les contrôler. Après que les membres de leur famille eurent été menacés, ils consentent à commettre une série d'actes qui pourrait se solder par un meurtre.

Rapport minoritaire (2002) – Inspiré d'une nouvelle de Phillip K. Dick, le film est projeté dans un futur où les policiers peuvent arrêter les crimes avant même qu'ils se produisent. Après qu'un policier est accusé d'un meurtre sur le point de survenir, le film porte sur l'influence de la surveillance sur la capacité des gens de faire des choix et d'assumer la responsabilité de leurs actes.

Red Road (2006) – L'opératrice d'une société de vidéosurveillance à Glasgow est habitée par l'obsession de suivre un homme qu'elle a aperçu sur ses écrans.

A Scanner Darkly (2006) – Inspiré du roman *Substance mort* de Phillip K. Dick, ce film explore l'utilisation de la surveillance dans un avenir dystopique dans lequel l'État a perdu la guerre contre la drogue.

La vengeance dans la peau (2007) – Un super soldat qui a perdu la mémoire s'évertue à échapper à la surveillance attentive de l'agent de la CIA qui l'a créé.

Foire aux questions sur la protection de la vie privée sur Internet

Dans cette annexe, vous trouverez les réponses aux questions les plus souvent posées sur la protection de la vie privée sur Internet. Comme les technologies Internet évoluent constamment, il est impossible de concevoir un guide complet sur les mesures de protection, mais les renseignements fournis dans cette annexe constituent un bon point de départ.

Les sites Web recueillent-ils des renseignements sur moi ?

La plupart le font. Certains sites Web énoncent leurs politiques très clairement et recueillent de l'information à votre sujet à diverses fins commerciales, notamment pour personnaliser les pages que vous consultez ou pour décider quelles publicités vous seront adressées. D'autres ensevelissent leurs politiques sous d'interminables et d'introuvables modalités tandis que d'autres amassent des renseignements personnels sans vous demander votre consentement ou vous permettre de refuser.

Parmi les renseignements que recueillent les sites Web, lesquels devraient m'inquiéter ?

Les sites Web peuvent recueillir votre nom, votre adresse physique, votre numéro de téléphone, les renseignements associés à votre carte de crédit, votre numéro d'assurance sociale, vos mots de passe, vos fichiers et vos dossiers personnels, vos activités en temps réels, votre emplacement, vos goûts et vos préférences. Vous fournissez certains de ces renseignements lorsque vous vous inscrivez à un service, mais certains renseignements pourraient être amassés sans que vous n'y consentiez ou que vous en ayez conscience.

Puis-je garantir la protection de mes renseignements personnels en ligne ?

Non. La seule chose que vous pouvez faire est de vous tenir au fait des mesures (présentées dans les paragraphes suivants) qui permettent de réduire le risque d'atteinte à la vie privée.

Suis-je protégé d'une atteinte à ma vie privée en ligne si je ne stocke des renseignements personnels que sur mon ordinateur et que je ne publie aucun renseignement en ligne ?

Pas nécessairement. Si vous n'avez pas configuré les paramètres de sécurité de votre ordinateur, il se peut qu'un tiers ait accès à vos renseignements et les télécharge sur un site public sans avoir votre consentement. Cette situation peut survenir lorsque vous ouvrez une pièce jointe à un courriel ou que vous installez un logiciel. Par ailleurs, certains lecteurs de musique, calendriers ou gestionnaires de photo permettent de faire un tri de vos fichiers sur votre ordinateur, mais ils peuvent également glaner de l'information sur votre ordinateur, la stocker ou la vendre à des tiers.

Comment fonctionnent les fichiers de témoins et devrais-je m'en inquiéter ?

Les fichiers de témoins sont de petites chaînes de codage informatique qui servent à stocker de l'information à votre sujet sur votre ordinateur. Ils peuvent ainsi vous identifier lorsque vous consultez de nouveau un site Web.

La façon la plus facile de déterminer si vous êtes suivi par des fichiers de témoins est si, lorsque vous consultez de nouveau un site Web, des détails comme vos préférences personnelles et de l'information sur votre profil apparaissent sans que vous ayez besoin de vous identifier. Sur les sites Web que vous visitez souvent, certains fichiers de témoins rendent la navigation plus facile puisqu'ils se souviennent de renseignements sur vous (nom et mot de passe) afin que vous n'ayez pas besoin de saisir ces renseignements chaque fois. Les sites de magasinage en ligne, les moteurs de recherche et les sites de partage de vidéo utilisent les fichiers de témoins pour personnaliser vos résultats de recherche et choisir des publicités qui devraient vous intéresser. De la même façon, certains fournisseurs de courrier électronique adaptent les publicités qui apparaissent sur votre écran au moyen du contenu de vos courriels. Si vous le souhaitez, vous pouvez désactiver les fichiers de témoins dans votre navigateur et ainsi empêcher ces sites de stocker ces fichiers dans votre ordinateur.

Comment puis-je réduire le suivi de mes activités en ligne ?

- Vous pouvez gérer les fichiers de témoins. Bien que vous ne puissiez pas consulter certains sites Web si vous avez désactivé les fichiers de témoins, pensez-y à deux fois avant d'accorder cette permission. Tous les navigateurs Web vous permettent de désactiver les fichiers de témoins. De plus, certains offrent même une fonction de « navigation privée » qui empêche ces fichiers d'être enregistrés.
- Vous pouvez supprimer les autres technologies de suivi de vos dernières séances de navigation au moyen de logiciel tiers. Le Commissariat à la protection de la vie privée prône l'utilisation de mécanismes « Do Not Track », une technologie d'interdiction de suivi qui permet aux gens de refuser l'essentiel du suivi en ligne ; ces mécanismes ne permettent toutefois pas d'empêcher tout le suivi en ligne.
- Vous pouvez utiliser plusieurs comptes courriel. Votre compte principal doit être associé à votre vrai nom et ne servir qu'aux communications avec des personnes que vous connaissez ou avec des groupes qui sont réservés aux membres seulement. Si vous prenez part à des discussions sur des forums ou des clavardages,

vous devriez employer une adresse secondaire associée à un pseudonyme. Le nom et l'adresse que vous indiquez sur les sites publics sont souvent recueillis et ciblés par les polluposteurs.
- Vous pouvez utiliser des moteurs de recherche qui ne recueillent pas vos renseignements personnels, comme StartPage.

Qu'est-ce que l'hameçonnage et comment puis-je en diminuer les risques ?

L'hameçonnage est une technique utilisée par les fraudeurs par laquelle ils se font passer pour un organisme légitime et demandent des renseignements personnels. La demande peut prendre la forme d'une fenêtre contextuelle, d'un site Web falsifié ou d'un courriel. Par exemple, un fraudeur peut vous demander de répondre à des questions communes pour la récupération d'un mot de passe. Quelle est votre date de naissance ? Quel est le nom de jeune fille de votre mère ? Quel est le nom de votre animal de compagnie ? Certaines autres méthodes d'hameçonnage consistent à vous faire cliquer sur un lien ; si vous le faites, un logiciel malveillant qui donne accès au fraudeur à vos renseignements de nature délicate, comme vos mots de passe ou vos renseignements bancaires, est installé automatiquement sur votre ordinateur. Pour atténuer les risques d'hameçonnage :

- Évitez d'ouvrir les courriels qui semblent suspects (ils se trouvent généralement dans le fichier de « pourriels » ou de courriels « indésirables »).
- Ne cliquez jamais sur les liens dans les courriels et les sites Web suspects.
- Mettez à jour votre navigateur ; vous aurez ainsi accès aux dernières fonctions de protection.
- Assurez-vous que votre connexion Internet est sécurisée ou embrouillée en vérifiant si l'adresse commence par « https » plutôt que par « http ». Le cadenas ouvert ou fermé dans la barre d'adresse ou dans un coin en bas de l'écran indique également si la page Web est sécurisée.
- Informez-vous sur les « extensions » de votre navigateur. Il existe plusieurs applications offertes qui vous permettent de chiffrer les sites Web que vous visitez et ainsi réduire les risques d'hameçonnage.

Comment puis-je protéger ma vie privée dans les médias sociaux ?

Les sites de médias sociaux font maintenant partie de notre quotidien. Bon nombre de gens mettent à jour leurs goûts, leurs préférences et le lieu où ils se trouvent en temps réel et dévoilent leurs allégeances politiques, leurs croyances religieuses et leurs vues sur des enjeux sociaux. En rendant ces renseignements publics, vous augmentez le risque que des tiers, comme des employeurs ou des voleurs d'identité, amassent vos renseignements personnels.

Pour mieux vous protéger dans les médias sociaux :

- Utilisez les paramètres de sécurité pour restreindre l'accès à vos renseignements personnels.
- Vérifiez régulièrement la politique sur les renseignements personnels du site de réseautage social que vous utilisez pour prendre connaissance des mises à jour et modifier les paramètres de sécurité au besoin. Cette mesure est très importante puisque nombre de médias sociaux mettent régulièrement à jour leurs politiques sur la protection des renseignements personnels sans informer leurs utilisateurs des changements apportés.
- Demandez-vous si vous pourriez regretter d'avoir publié une photo ou un commentaire dans quelques jours ou dans quelques années ? Pour prendre les décisions d'embauche, les employeurs se fient souvent aux renseignements qu'un candidat potentiel a dévoilés lui-même sur sa vie publique privée dans les médias sociaux. Évitez donc de publier des choses qui pourraient revenir vous hanter.
- Avant de publier une photo ou un commentaire sur une personne, vérifiez avec elle au préalable. Ne présumez pas que du contenu qui semble insignifiant pour vous ne gênera pas ou ne choquera pas une autre personne. Vous encouragerez ainsi les autres à vous traiter de la même façon.
- Si une personne a publié des détails sur vous et que vous vous sentez gêné, demandez-lui de les supprimer. Bien que cette information puisse être conservée par le site du réseautage social, en la supprimant vous réduisez le risque que d'autres personnes y aient accès facilement.

En quelles connexions Internet puis-je avoir confiance ? Comment puis-je faire pour protéger ma connexion ?

La connexion Internet la plus sûre est habituellement celle que vous avez à la maison, parce qu'en général, moins de personnes l'utilisent. Voici quelques façons de rendre votre expérience virtuelle plus sûre :

- Mettre fréquemment à jour votre clé de réseau (mot de passe pour vous connecter au réseau) et utiliser une combinaison aléatoire de lettres, de signes de ponctuations, de symboles et de chiffres.
- Utiliser du matériel et un logiciel pare-feu efficaces pour réduire votre vulnérabilité aux pirates informatiques.
- Désactiver votre connexion Internet lorsque vous ne l'utilisez pas. Les pirates informatiques recherchent les connexions Internet non surveillées pour accéder aux renseignements sur les cartes de crédit ou d'autres renseignements de nature délicate.
- Réfléchir aux sites Web que vous visitez au travail par rapport à ceux que vous consultez à la maison. La surveillance permet notamment aux employeurs de consigner et de voir tout le contenu Internet envoyé à partir d'un poste de travail. Même si vous effacez un fichier de votre ordinateur au travail, votre directeur pourrait être capable de le voir en aval.

Comment puis-je protéger mon enfant quand il navigue sur Internet ?

- Informez-vous sur les risques auxquels s'exposent les enfants en ligne. Consultez le site MediaSmarts.ca pour en apprendre plus sur la protection de la vie privée en ligne, le contenu obscène, la cyberintimidation et le vol d'identité.
- Parlez avec votre enfant des problèmes auxquels il pourrait se heurter et des types de sites Web qu'il devrait consulter. Vous pouvez installer un logiciel de contrôle parental pour bloquer le contenu que vous jugez inapproprié directement dans votre navigateur ou par l'intermédiaire de votre fournisseur Internet. Vous devez toutefois faire preuve de prudence avec ces logiciels. La meilleure façon de protéger votre enfant dans le monde virtuel

est de parler avec lui, de lui signifier clairement vos attentes et de compter sur le fait qu'il viendra vous voir s'il commet une erreur.

- Établissez un lien de confiance avec votre enfant ; c'est la chose la plus importante à faire. Si vous tentez de le surveiller plutôt que de communiquer, vous pourriez obtenir l'effet contraire. En utilisant un logiciel de contrôle parental, en insistant pour que votre enfant accepte votre demande d'amitié sur Facebook ou en lui demandant qu'il vous donne le mot de passe de son compte dans les médias sociaux ou de son téléphone cellulaire, vous ferez en sorte que votre enfant soit moins porté à venir vous voir s'il a un problème, plus particulièrement si votre enfant approche de l'adolescence.
- Pensez à avoir une discussion sur les « conversations avec les inconnus » avec votre enfant lorsqu'il est jeune, bien que la majorité des enfants ne parlent qu'avec des gens qu'ils connaissent. Enseignez à votre enfant à prendre quelques précautions, comme utiliser un pseudonyme, ne jamais communiquer son numéro de téléphone, son adresse ou son emplacement, ne pas publier de photos et ne jamais accepter de rencontrer quelqu'un sans avoir la permission ou sans supervision.
- Encouragez votre enfant à vous faire part de ses opinions en usant de moyens constructifs et créatifs. Rappelez-lui que les professeurs ou de futurs employeurs pourraient voir ce qu'il publie.
- Faites savoir à votre enfant qu'il peut venir vous voir s'il voit des commentaires racistes, homophobes ou misogynes, des propos haineux, etc.
- Discutez avec vos préadolescents et vos adolescents des conséquences du sextage, c'est-à-dire de l'envoi de messages à caractère sexuel ou de photos de nudité ou de nudité partielle d'eux ou d'autres personnes sur Internet ou avec leur téléphone cellulaire. Dès que l'enfant appuie sur « envoyer », il pourrait très facilement ne plus avoir le contrôle sur qui peut voir cette image.
- Encouragez votre enfant à se tourner vers vous s'il a besoin d'aide, si quelqu'un a publié du contenu blessant, gênant et choquant à son sujet. Aidez votre enfant à trouver des stratégies, comme confronter face-à-face ou demander à la personne de supprimer le contenu. Si la situation est grave, demandez à votre enfant s'il

veut que vous discutiez du problème avec les parents de l'autre enfant ou avec le directeur de l'école.

Les lois canadiennes peuvent-elles m'aider à protéger mon information des entreprises en ligne ?

Oui, elles le peuvent. Veuillez vous reporter à l'Annexe 1 pour plus de renseignements.

Quels sont mes recours si l'on a porté atteinte à ma vie privée en ligne ?

Si vous soupçonnez que certains renseignements personnels ont été compromis (comptes bancaires), contactez immédiatement l'institution concernée (banque ou société d'appréciation de la solvabilité) pour vous protéger contre le vol d'identité. Le Commissariat à la protection de la vie privée peut également vous aider dans les cas suivants :

- Vous croyez que votre information personnelle est utilisée, recueillie ou communiquée de façon inadéquate.
- Vous avez de la difficulté à faire en sorte qu'un organisme corrige des renseignements inexacts à votre sujet.
- Vous avez demandé à un organisme quels renseignements personnels il détient sur vous et celui-ci refuse de vous y donner accès.

Organisations non gouvernementales canadiennes œuvrant dans le domaine de la surveillance, de la protection de la vie privée et des libertés civiles

British Columbia Civil Liberties Association

- Site Web : bccla.org *(en anglais seulement)*
- Emplacement : Vancouver
- Année de fondation : 1962
- Mission officielle : Plus ancien groupe des droits civils au Canada, cette Association a pour mandat de préserver, défendre, maintenir et augmenter les droits civils et les droits de la personne au Canada.
- Activités : Défense-action, politique publique, éducation communautaire et programmes en matière de justice.

British Columbia Freedom of Information and Privacy Association

- Site Web : fipa.bc.ca *(en anglais seulement)*
- Emplacement : Vancouver
- Année de fondation : 1991
- Mission officielle : L'Association a pour objectifs de faire la promotion et défendre l'accès à l'information et le droit à la vie privée au Canada et de donner des moyens d'agir aux citoyens

en augmentant leur droit d'accès à l'information détenue par le gouvernement, en faisant la promotion du principe d'accès universel et abordable aux modes de communication de base à notre époque, en restreignant les activités de surveillance de l'État et en renforçant le droit d'accès à nos renseignements personnels ainsi que notre capacité de contrôler la collecte, l'utilisation et le partage de nos renseignements personnels lorsqu'ils sont consignés.
- Activités : Offrir des services à diverses personnes et à un éventail d'organismes au moyen de programme d'éducation et d'aide au public, de recherche et de réforme du droit.

Association canadienne des libertés civiles

- Site Web : ccla.org
- Emplacement : Toronto
- Année de fondation : 1964
- Mission officielle : Faire la promotion du respect des droits fondamentaux de la personne et des libertés civiles ; défendre ces droits et ces libertés et en favoriser la reconnaissance.
- Activités : Les travaux de l'Association portent principalement sur les domaines suivants : libertés fondamentales, sécurité publique, sécurité nationale et égalité. L'Association a mis au point un modèle unique de défense des intérêts qui concourt à cinq activités de base : éducation du public, mobilisation citoyenne, recherche et litige.

Clinique d'intérêt public et de politique d'Internet du Canada

- Site Web : cippic.ca
- Emplacement : Ottawa
- Année de fondation : 2003
- Mission officielle : La mission de la CIPPIC comporte deux volets : (a) remplir les vides dans le débat sur les politiques publiques, notamment sur les questions de droit relatives à la technologie, assurer un équilibre entre les processus de confection des politiques et des lois et offrir de l'aide juridique aux organismes et aux

personnes sous représentés dans les dossiers qui sont à l'intersection de la loi et de la technologie ; (b) offrir aux étudiants en droit une formation en droit de grande qualité et gratifiante.
- Activités : Recherche, production de rapports et présentation au gouvernement, formulation d'observations sur les projets de réforme législative, prestation de conseils juridiques aux particuliers et aux organismes, et mise au point de ressources en ligne à l'intention du public portant sur les enjeux juridiques découlant des nouvelles technologies.

Coalition pour la surveillance internationale des libertés civiles

- Site Web : iclmg.ca
- Emplacement : Ottawa
- Année de fondation : 2001
- Mission officielle : Défendre les libertés civiles et les droits de la personne énoncés dans la *Charte canadienne des droits et libertés*, les lois fédérales et provinciales et les instruments internationaux relatifs aux droits humains.
- Activités : Suivi de l'évolution et de l'application des priorités du Canada concernant les mesures de sécurité et antiterroriste, sensibilisation du public aux conséquences des lois et d'autres mesures antiterroristes, travail de lobbying et la réalisation de travaux de plaidoyer, et appui aux efforts internationaux visant à atténuer l'incidence des lois sur la sécurité adoptées par le Canada ou les autres pays avec qui le Canada harmonise ses politiques de sécurité à l'échelle internationale.

La Ligue des droits et libertés

- Site Web : liguedesdroits.ca
- Emplacement : Ottawa
- Année de fondation : 1963
- Mission officielle : Faire connaître, défendre et promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la *Charte internationale des droits de l'Homme*.

- Activités : Collaborer avec le gouvernement et d’autres organismes, tant à l’échelle nationale qu’internationale, dénoncer les cas de violations des droits de la personne. Mener des activités de sensibilisation et de formation pour parler le plus possible des droits qui touchent tous les aspects de la vie en société.

OpenMedia.ca

- Site Web : openmedia.ca *(en anglais seulement)*
- Emplacement : Vancouver
- Année de fondation : 2008
- Mission officielle : Donner les moyens aux gens de participer à la gouvernance Internet au moyen de campagnes originales et faisant participer les citoyens. OpenMedia.ca est un réseau d’organismes qui collaborent en vue de promouvoir les principes suivants : l’accès, le choix, la diversité, l’innovation et l’ouverture.
- Activités : Mobiliser, éduquer et donner les moyens d’agir aux citoyens en vue de défendre et de faire progresser leurs intérêts, leurs valeurs et leurs droits en matière de communication. OpenMedia.ca mobilise les citoyens au moyen de campagnes électroniques et d’événements participatifs qui parlent aux gens ordinaires ; il encourage également l’engagement civique dans les médias et les politiques de communication au Canada ; il fait de la sensibilisation au moyen d’événements et de ressources électroniques et donne les moyens d’agir par des outils en ligne et des processus ouverts qui permettent aux citoyens de mettre de l’avant leur vision des médias ouverts.

Centre pour la défense de l’intérêt public

- Site Web : piac.ca *(en anglais seulement)*
- Emplacement : Ottawa
- Année de fondation : 1976
- Mission officielle : Le Centre est un organisme à but non lucratif qui offre des conseils juridiques et des services de recherche pour défendre les consommateurs, en particulier les consommateurs

vulnérables, en ce qui concerne la prestation des services publics de premier ordre.
- Activités : Recherche en droit, défense des consommateurs, éducation et lobbying.

Conseil du Canada de l'accès et de la vie privée

- Site Web : pacc-ccap.ca *(en anglais seulement)*
- Emplacement : Calgary
- Année de fondation : 2002
- Mission officielle : Mieux faire connaître l'accès à l'information, la protection de la vie privée et la gouvernance de l'information et en faire la promotion.
- Activités : Défense des intérêts, sensibilisation, éducation, formation et mobilisation citoyenne. Le Conseil gère un programme de certification professionnelle conforme aux normes nationales de compétence, de professionnalisme et de connaissances.

Rocky Mountain Civil Liberties Association

- Site Web : rmcla.ca *(en anglais seulement)*
- Emplacement : Calgary
- Année de fondation : 2009
- Mission officielle : Promouvoir le respect des droits fondamentaux de la personne et des libertés civiles et défendre et assurer leur protection.
- Activités : Protéger la liberté d'expression au moyen de modifications à la *Human Rights Act* de l'Alberta, améliorer l'éducation sur les droits de la personne et la discrimination liée à la grossesse et faire progresser les dossiers concernant l'accès à la justice.

Vancouver Public Space Network

- Site Web : vancouverpublicspace.wordpress.com *(en anglais seulement)*

- Emplacement : Vancouver
- Année de fondation : 2006
- Mission officielle : S’efforcer de défendre l’importance de l’espace public pour la qualité de vie de la ville.
- Activités : Défense des intérêts, éducation et sensibilisation au domaine public à Vancouver. Le Vancouver Public Space Network vise à offrir un amalgame de recherche ciblée et de travail de conception, de mobilisation communautaire créative et d’une approche constructive axée sur les solutions.

Suggestions de lecture

Ouvrages généraux

Ball, Kirstie, David Lyon et Kevin Haggerty. *The Routledge Handbook of Surveillance Studies.* Londres et New York, Routledge, 2012.

Ce vaste recueil d'essais fait un tour d'horizon complet des études sur la surveillance. Il comprend cinquante textes écrits par des grandes figures du domaine et contribuera à définir l'étude de la surveillance pour les années à venir.

Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance.* Cambridge, MA, MIT Press, 2008.

Colin J. Bennett se penche sur le vaste réseau de « défenseurs du droit à la vie privée » dans le contexte plus large de la politique de la surveillance et du droit à la vie privée. Il expose en détail les divers rôles que ces personnes peuvent jouer, de défenseur à chercheur en passant par consultant, et présente les nombreux défis auxquels ils doivent faire face pour contester l'expansion de la surveillance.

Cole, Simon A. *Suspect Identities: A History of Fingerprinting and Criminal Identification,* Cambridge, MA, Harvard University Press, 2001.

Simon A. Cole fait un bilan réfléchi de l'avènement historique et des utilisations modernes des empreintes digitales. Dans son livre, il expose les premières difficultés rencontrées pour convaincre les autorités que les empreintes digitales permettent la personnalisation, les utilisations coloniales des empreintes et les enjeux contemporains liés à leur exactitude. Le dernier chapitre porte sur les liens de l'analyse d'ADN avec l'histoire de l'identification personnalisée.

Funder, Anna. *Stasiland : Où nous sommes tous suspects*, traduit de l'anglais par Mireille Vignol, Éditions Héloïses d'Ormesson, Paris, 2008, 368 pages.
Ces mémoires troublantes font état de l'héritage déconcertant laissé par la surveillance effectuée par le Ministère de la sécurité d'État (Stasi). L'ouverture des archives secrètes a permis de mettre en lumière les pratiques de surveillance de l'État et de permettre aux gens de connaître qui de leurs amis, des membres de leur famille et de leurs collègues étaient des informateurs à leur sujet.

Gilliom, John. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*, Chicago, University of Chicago Press, 2001.
Dans ce livre, John Gilliom nous livre une étude touchante sur la façon dont les femmes de la région des Appalaches aux États-Unis sont surveillées dans les moindres détails par un système informatique perfectionné d'aide sociale. Il met l'accent sur les problèmes auxquels se heurtent quotidiennement les bénéficiaires de l'aide sociale et la résistance qu'ils y opposent.

Gilliom, John et Torin Monahan. *SuperVision: An Introduction to the Surveillance Society*, Chicago, University of Chicago Press, 2012.
Cet ouvrage dense sert d'introduction générale aux études sur la surveillance. Les auteurs y analysent les mécanismes manifestes de surveillance, comme les caméras de CCTV et les mesures de sécurité dans les aéroports. De plus, ils explorent également le potentiel de surveillance des technologies qui ont maintenant envahi notre quotidien (téléphone cellulaire, carte de crédit, Internet et GPS) et examinent les conséquences éthiques et politiques de ces technologies.

Hier, Sean P. *Panoptic Dreams: Streetscape Video Surveillance in Canada,* Vancouver, University of British Columbia Press, 2010.

Cet ouvrage présente l'examen le plus complet ayant été fait sur l'avènement des caméras de surveillance au Canada. L'auteur présente une analyse détaillée des enjeux politiques entourant l'installation de ces caméras dans différentes villes et municipalités au Canada. Il soulève également des questions quant à l'efficacité des caméras dans la lutte contre la criminalité.

Laidler, Keith. *Surveillance Unlimited: How We've Become the Most Watched People on Earth*, Cambridge, Royaume-Uni, Icon, 2008.

Dans ce livre, l'auteur parle de la situation en Grande-Bretagne en explorant les nouveaux outils de surveillance, comme les nouvelles formes d'identification parrainées par l'État, l'identification par radiofréquence et les caméras de surveillance. Il se penche sur la réaction sur le plan politique et pragmatique que pourraient avoir les citoyens concernés par ces nouveautés.

Lyon, David. *Surveillance Studies: An Overview,* Cambridge, Royaume-Uni, Polity Press, 2007.

Dans cet ouvrage, l'auteur analyse les diverses questions étudiées dans le cadre des études sur la surveillance. Les lecteurs qui s'intéressent à la réflexion de l'auteur pourraient lire également *The Electronic Eye* (1994) et *Surveillance Society* (2001).

Marx, Gary T. *Undercover: Police Surveillance in America*, Berkeley, University of California Press, 1988.

Cette étude encensée sur les pratiques de la police secrète porte sur les aspects pratiques et l'éthique de ces méthodes. Le dernier chapitre intitulé « The New Surveillance » (la nouvelle surveillance) est un point de référence inévitable puisque l'auteur y prévoit la montée des nouvelles formes de surveillance électronique.

Mayer-Schönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age,* Princeton, Princeton University Press, 2009.

La révolution numérique signifie que des rames d'information qui, à d'autres époques, se seraient évaporées sont maintenant conservées à perpétuité sur divers systèmes électroniques. Ce nouveau phénomène a des conséquences sur la mémoire sociale, mais également sur la

scène politique puisque les gens ne peuvent plus réellement s'attendre à ce que leurs gestes et leurs actions passés soient oubliés.

Nippert-Eng, Christena. *Islands of Privacy,* Chicago, University of Chicago Press, 2010.

L'auteure fait le bilan des entrevues qu'elle a effectuées auprès de résidents de Chicago au sujet de leurs vues sur la vie privée et du secret des communications. La principale leçon que nous apprend cet ouvrage est que la vie privée est toujours au cœur des comportements humains et que les gens déploient des efforts considérables pour protéger leur vie privée.

Norris, Clive et Gary Armstrong. *The Maximum Surveillance Society: The Rise of CCTV,* Oxford, Berg, 1999.

Cet ouvrage est l'une des premières et des meilleures analyses sur l'utilisation des caméras de surveillance en Angleterre. Les auteurs y fournissent d'excellents renseignements qu'ils ont obtenus en passant beaucoup de temps dans une centrale de surveillance, et en observant et en consignant les diverses formes (parfois douteuses) de déviance que les opérateurs voient et ignorent.

O'Harrow, Robert, Jr. *No Place to Hide,* New York, Free Press, 2005.

O'Harrow, un reporter pour le *Washington Post*, fait un travail admirable en personnalisant la portée de l'information recueillie à des fins commerciales. Ce livre dévoile des détails troublants sur les façons souvent cyniques qu'emploient les grandes sociétés de l'information pour miner la vie privée.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff Between Privacy and Security,* New Haven, Yale University Press, 2012.

Dans cet ouvrage, l'auteur explique ce qu'est la protection de la vie privée et s'il est vraiment nécessaire de compromettre la vie privée pour la sécurité. Il explique comment la loi protège la vie privée et se penche sur les préoccupations relatives aux nouvelles technologies et l'échec de notre système actuel. Il suggère même des solutions.

Turow, Joseph. *The Daily You: How the Advertising Industry Is Defining Your Identity and Your Worth,* New Haven, Yale University Press, 2012.

Dans cet ouvrage, l'auteur se penche sur la façon dont les publicitaires suivent les utilisateurs sur les sites Web afin de présenter des publicités qui – ils le souhaitent – façonneront le comportement des consommateurs. L'auteur soulève des questions au sujet des conséquences politiques puisque cette façon de faire pourrait bien réduire l'éventail d'information auquel les citoyens consommateurs sont exposés.

Fiction

Asimov, Isaac. *Le cycle de fondation* (1951-1953).

Asimov nous présente un traitement classique de la puissance des prévisions. Hari Seldon tente d'éviter l'âge des ténèbres intergalactique en appliquant la science de la psychohistoire, une branche des mathématiques qui peut prédire l'avenir en surveillant et en analysant le comportement d'une foule de gens équivalente à la population de la galaxie.

Dick, Philip K. *Substance mort* (1977).

Dans ce roman, Dick fait une critique pertinente de l'interaction entre l'anonymat, la technologie et l'application de la loi. Dans un futur dystopique, un policier infiltré s'habille d'un « costume brouillé » pour cacher son identité pendant qu'il part à la recherche de la source d'une nouvelle drogue très dangereuse.

Eggers, Dave. *The Circle* (2013).

Mae, âgé d'une vingtaine d'années, est embauché par The Circle, un conglomérat d'entreprises de recherche en ligne ainsi que de médias sociaux et d'autres sociétés Internet de Silicon Valley qui a comme objectif une transparence totale, mondiale et 24 heures par jour. Dans son roman, Eggers crée un monde numérique dystopique qui touche à l'appropriation de plus en plus grande de la vie privée par les entreprises privées par des slogans orwéliens du type « les secrets sont des mensonges » et « la vie privée est un vol ».

Gibson, William. *Neuromancien* (1984).

Ce roman est l'histoire d'un pirate informatique de génie épuisé qui est embauché par un employeur mystérieux pour l'attaque informatique du siècle. Avec cet ouvrage qui fait partie de la trilogie composée de *Neuromancien, Comte Zéro* et *Mona Lisa s'éclate*, Gibson est devenu le père de la génération cyberpunk et a popularisé le mot cyberespace en examinant les communautés virtuelles, l'espace et l'intelligence artificielle.

Huxley, Aldous. *Le meilleur des mondes* (1932).

Huxley fait dans ce livre une critique brillante de la société de consommation. Dans un futur dystopique, la reproduction naturelle a été mise de côté et les consommateurs-citoyens sont manipulés par l'État au moyen d'hallucinogènes et du conditionnement du comportement. Contrairement au régime totalitaire du Big Brother d'Orwell, le gouvernement de l'année 634 AF (Après Ford) contrôle ses sujets en surveillant la consommation et en détruisant l'individualité.

Orwell, George. *1984* (1949).

Ce classique d'Orwell constitue toujours une référence dans les discussions sur la surveillance. D'autres romans ont abordé le thème d'une surveillance coercitive pouvant être faite par l'État, mais aucun n'a autant fait parler en présentant la notion de « Big Brother ».

Collaborateurs

Colin Bennett est professeur au Département de sciences politiques de l'Université de Victoria. Ses recherches sont axées sur l'analyse comparative des technologies de la surveillance et des politiques de protection de la vie privée à l'échelle nationale et internationale. En plus des nombreux articles scientifiques et des articles de journaux qu'il a publiés, il a écrit six livres dont *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2008), et des rapports sur les politiques relatives à la protection de la vie privée pour des organismes canadiens et étrangers. Il est actuellement chercheur associé dans le cadre du projet sur la Nouvelle transparence : la surveillance et le tri social des Grands travaux de recherche concertée.

Andrew Clement est professeur à la Faculté de l'information à l'Université de Toronto ; il y coordonne le programme de recherche sur la politique de l'information et est cofondateur de l'Identity, Privacy and Security Institute. Il est titulaire d'un doctorat en informatique et fait de la recherche depuis longtemps sur l'incidence sociale des technologies de l'information et de communication et la mise au point de systèmes d'information axés sur le facteur humain et participatif. Parmi les projets de recherche sur la surveillance auxquels il a participé récemment, citons le IXmaps.ca, un outil de cartographie Internet qui contribue à rendre plus visibles les activités de branchement clandestin que mène sans mandat la National Security Agency des États-Unis. Il est actuellement chercheur associé dans le cadre du projet sur la Nouvelle transparence : la surveillance et le tri social des Grands travaux de recherche concertée.

Arthur Cockfield est professeur à la Faculté de droit de l'Université Queen's où il a été nommé boursier national. Avant de se joindre à l'Université Queen's, il a travaillé comme avocat à Toronto et comme professeur de droit à San Diego. Il est un chercheur supérieur attaché à l'Université Monash de Melbourne, en Australie, et il a été chercheur à la chaire de chercheurs invités de Fulbright pour l'étude des politiques à l'Université du Texas à Austin au printemps 2013. Les recherches de Cockfield portent principalement sur le droit fiscal, le droit relatif au respect de la vie privée et la théorie du droit ainsi que des technologies.

Aaron Doyle est professeur agrégé au Département de sociologie et d'anthropologie de l'Université Carleton. Ses recherches sont axées sur la façon dont les institutions, comme les médias, le système de justice pénale et les organismes d'assurance, gèrent les risques au moyen, entre autres, de la surveillance ainsi que les garanties et les insécurités qui en découlent. Il a rédigé, corédigé et copublié de nombreux articles et sept livres dans le domaine, dont le plus récent est *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge, 2012), publié également sous la direction de Randy Lippert et David Lyon.

Kevin D. Haggerty est l'éditeur des *Cahiers canadiens de sociologie* et est professeur de sociologie et de criminologie à l'Université de l'Alberta. Ses derniers travaux portent sur la surveillance, la gouvernance, le maintien de l'ordre et les risques. Aaron Doyle et lui collaborent actuellement à la rédaction d'un livre intitulé *65 Ways to Screw Up in Graduate School*, par lequel ils souhaitent transmettre une série de leçons professionnelles à la prochaine génération d'étudiants des cycles supérieurs.

Stéphane Leman-Langlois est professeur agrégé en criminologie à l'Université Laval. Il est actuellement titulaire de la chaire de recherche du Canada en surveillance et construction sociale du risque, qui administre le Laboratoire de surveillance virtuelle (LSV), un environnement 3D expérimental pour l'étude des conséquences comportementales de la surveillance. Parmi les livres qu'il a publiés récemment, mentionnons *Technocrime: Policing and Surveillance* (Routledge, 2012), *Sphères de surveillance* (Presses de l'Université de Montréal, 2011), *Terrorisme et antiterrorisme au Canada* (Presses de l'Université de Montréal, 2009), et *Technocrime: Technology, Crime and Social Control* (Willan Publishing, 2008).

David Lyon est directeur du Centre des études sur la surveillance de l'Université Queen's, titulaire de la chaire de recherche de l'Université Queen's sur les études sur la surveillance et professeur au Département de sociologie et à la Faculté de droit de l'Université Queen's. Depuis 2008, il dirige l'équipe du projet sur la Nouvelle transparence : la surveillance et le tri social, qui a produit cet ouvrage. Parmi les livres qu'il a publiés récemment, citons *Liquid Surveillance* (en collaboration avec Zygmunt Bauman ; Polity Press, 2013), *The Routledge Handbook of Surveillance Studies* (publié également sous la direction de Kirstie Ball et Kevin Haggerty ; Routledge, 2012), *Identifying*

Citizens: ID Cards as Surveillance (Polity Press, 2009), et *Surveillance Studies: An Overview* (Polity Press, 2007). Il est cofondateur de journal *Surveillance and Society* et du Surveillance Studies Network.

Benjamin J. Muller est professeur agrégé en sciences politiques au King's University College et est membre du corps enseignant du Centre d'études américaines de la Western University. Il est l'auteur de plusieurs articles et de chapitres dans le domaine des études critiques sur la sécurité, des études sur la surveillance et de la sociologie politique internationale ; il se concentre particulièrement sur les frontières, les régions frontalières, la sécurité et les technologies biométriques. Parmi ses publications, citons *Security, Risk, and the Biometric State: Governing Borders and Bodies* (Routledge, 2010) et *Rethinking Hizballah: Legitimacy, Authority, Violence* (en collaboration avec Samer N. Abboud ; Ashgate, 2012).

David Murakami Wood est titulaire de la Chaire de recherche du Canada en études sur la surveillance (niveau 2) à l'Université Queen's. Il a publié de nombreux articles et est un expert en sociologie, en géographie de la surveillance et en perspectives comparatives mondiales en matière de sécurité urbaine. Il se concentre notamment sur le Japon, le Brésil, le Canada et le Royaume-Uni. Il est cofondateur et rédacteur en chef de journal *Surveillance and Society* et cofondateur du Surveillance Studies Network.

Laureen Snider est professeure en sociologie à la retraite de l'Université Queen's. Elle se spécialise dans la criminalité d'entreprise, la surveillance et la réforme judiciaire. Parmi ses publications récentes, mentionnons *The Surveillance-Industrial Complex: A Political Economy of Surveillance* (en collaboration avec Kirstie Ball ; Routledge, 2013) ; « The 'Great Unwatched' and the 'Lightly Touched' » (en collaboration avec Adam Molnar), le chapitre 8 de l'ouvrage *The Surveillance-Industrial Complex* (Routledge, 2013) ; « The Technological Advantages of Stock Market Traders », chapitre 8 de *How They Got Away with It: White Collar Criminals and the Financial Meltdown* (Columbia University Press, 2013) ; « The Conundrum of Financial Regulation » dans l'*Annual Review of Law and Social Sciences* (2011) ; et « Examining the Ruggie Report: Can Voluntary Guidelines Tame Global Capitalism? » (en collaboration avec Steven Bittle), dans *Critical Criminology* (2013).

Valerie Steeves est professeure agrégée au Département de criminologie de l'Université d'Ottawa. Elle a fait de nombreux exposés et écrits de nombreux textes sur la protection de la vie privée. Elle est actuellement chercheuse principale dans le cadre du projet eGirls (financé par le Conseil de recherches en sciences humaines du Canada) ; elle y étudie notamment le rôle des genres dans les médias sociaux. Elle est également chercheuse principale dans le cadre du projet de recherche Jeunes Canadiens dans un monde branché (financé par le Commissariat à la protection de la vie privée du Canada).

Index